公開資料

（様式・終了－１）

社会技術研究開発事業
研究開発領域「情報と社会」
研究開発プログラム「ユビキタス社会のガバナンス」
研究開発プロジェクト「企業における情報セキュリティの実効性あるガバナンス制度のあり方」

研究開発実施終了報告書

研究開発期間　平成１９年７月～平成２１年１２月

研究代表者氏名　林 紘一郎
(情報セキュリティ大学院大学　学長・教授)

目　次

１．研究開発プロジェクト ····· 2
２．研究開発実施の概要 ····· 2
３．研究開発構想 ····· 5
４．　研究開発成果 ····· 7
第１編　総論編 ····· 8
1　課題の設定から仮説の定立に至るまで ····· 8
2　背景となる理論的研究 ····· 10
3　実証研究（詳細は「第３編　実証研究編」参照） ····· 18
4　経営層に向けた提言 ····· 19
5　個別提言 ····· 20
第２編　理論研究編 ····· 22
1　情報セキュリティとガバナンス ····· 22
2　情報セキュリティガバナンスにおける表示と法的責任 ····· 24
3　第三者評価認証制度 ····· 33
4　プライバシーマーク制度とその問題点 ····· 38
5　ISMS 適合性評価制度とその問題点～外部委託を中心に～ ····· 44
第３編　実証研究編 ····· 51
1　情報セキュリティのガバナンスと逸脱行動に関する調 ····· 51
2　ネットワークの情報流通と企業ガバナンスに関する調査 ····· 64
第４編　個別提言 ····· 74
1　ガバナンスのあり方に関する提言 ····· 74
2　シグナル情報のあり方に関する提言 ····· 82
3　情報と情報セキュリティの一般論に関する提言 ····· 89
５．研究開発実施体制 ····· 97
６．成果の発信やアウトリーチ活動など ····· 100
７．結び ····· 105

１．研究開発プロジェクト

(1)研究開発領域：情報と社会

(2)領域総括　　：土居 範久

(3)研究代表者　：林　紘一郎

(4)研究開発プロジェクト名:企業における情報セキュリティの実効性あるガバナンス制度のあり方

(5)研究開発期間：　平成１９年７月～平成２１年１２月

２．研究開発実施の概要

①　研究開発目標(アンダーラインの部分は、当初計画を微修正)

日々膨大な情報を取り扱いリスク･テイカーである企業を対象に、情報セキュリティを実効あらしめるために、いかなる「制度」が望ましいかという視点から、そのガバナンスのあり方を検討する。リスク類型別のケース・スタディにより、消費者の視点に立って問題点を摘出する。そして、誰がどのような責任を負うべきか、あるいは責任の追及よりも今後の改善策の検討により多くの資源を投入すべきか等について、判断基準を提供する。また判断基準が提供できないケースについては、その原因を明確にする。

②　研究開発項目、③実施内容

本格研究は、2007 年 7 月から開始した。法制度班及び経営管理班では、1 ヶ月～2 ヶ月に 1 度のペースで定期会合を実施し、適宜、技術班へのフィードバックを行ってきた。

経営管理班の関連では、情報システム利用者の意識を測るべく、2008 年度に、富士通総研㈱に情報セキュリティと「エンゲージメント」「ソーシャルキャピタル」に関する調査委託を行った。2009 年度は、その発展系として、「情報セキュリティのガバナンスと逸脱行動に関する調査」を委託した。技術班では、メールベースでの情報交換のほか、必要に応じて対面での打合せを行った。2008 年度には、(株)情報技研と委託契約を締結し、企業の対外通信データを収集・分析し、企業活動との相関を測るための調査を行った。2009 年度は、NTT-IT(株)の協力を得て、拡大調査を実施した。これらの調査は、理論研究を裏付けるものとして重要な位置を占めている。

その他、若手研究会の実施、3 ヶ月に 1 度の全体会合又はシンポジウムの実施、メンバーの出張、ヒアリング等を通じて、各班共通の問題意識の集約や、CIA に代わる新たな情報セキュリティの要素の検討等を行ってきた。

法制度班、経営管理班は、2008 年度末にそれぞれ検討結果の取りまとめを行い、活動を終了することとした。技術班も活動を終了したが、上記 2 つの調査は 2009 年度も継続して行った。

2009 年度は、最終報告書起草グループを新たに編成し、全体のとりまとめを行う総括班との二班体制で検討を進めた。

こうした活動の中では、様々な論点が取り上げられた。それらの経緯は、各年度の研究開発実施報告書に記載したとおりである。

④主な結果・成果

2年半の本格研究を通じて、3つの成果を得ることができた。

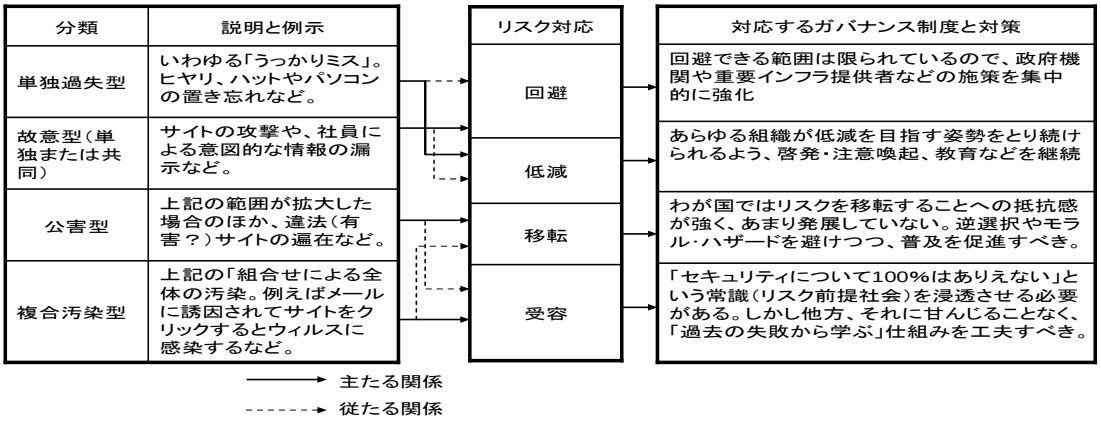
第１は、社会的アピールと情報セキュリティ文化の醸成のための社会的アピールである。

企業経営における情報セキュリティの重要性に関して、トップ・エグゼクティブ（特に文系出身者）が、以下 5 項目の認識を共有すべきであるという結論に到達した。これら 5 項目は、本研究から生まれる諸提言を理解していただくための、基礎となるとともに、わが国固有の情報セキュリティ文化の醸成に寄与するものである。

認識１．(リスク･テーカーとしての企業) 企業はリスク・テーカーであり、リスクを低減したり、ヘッジしたり、移転したりすることは出来るが、それをゼロにすることはできない。

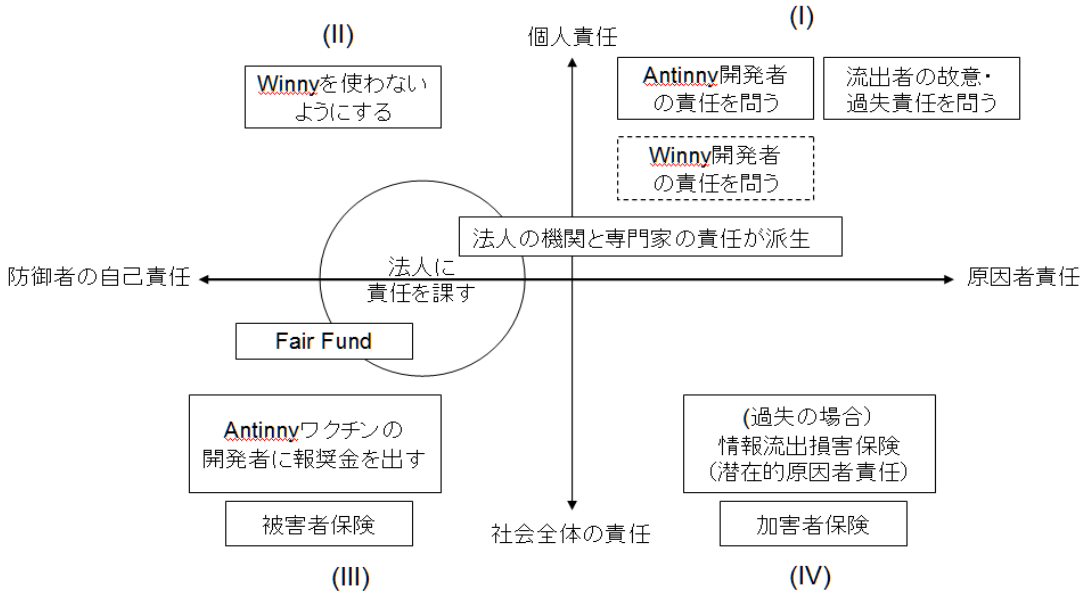
認識２．（業務のシステム依存）
企業活動の大部分は、コンピュータとネットワーク・システムに支えられており、そのリスク対策が情報セキュリティであるから、これは経営の根幹に触れる問題である。
認識３．（経営者自身に課せられた最適化問題）
情報セキュリティがリスク対策である以上、それは全社的に費用対効果を最適化すべきものであり、他の経営意思決定と何ら異なるものではない（専門家に任せておいて済むものではない）。
認識４．（ガバナンス制度間の整合性）
情報セキュリティ対策は、経営全般のガバナンスと責任のあり方（内部統制、コンプライアンス、品質管理、環境適応、企業の社会的責任）などと整合的、かつ統制の取れたものでなければならない。
認識５．（企業ごとの特色）
情報セキュリティ対策は、企業を取り巻く環境や、長年にわたって培われた企業文化と不可分のものであるから、他から移植して済むものではなく、自ら生み出さねばならない（わが国全体としてみれば、「日本的経営の特色」との整合性が必要である）。

第 2 は、インシデントの分類と責任のあり方を明らかにしたことである。研究開発目標を達成するために、個人情報漏えいやスパムメールなどのインシデントを分析し、リスク対応やガバナンス制度との間に、次表のような対応関係があることを解明した。



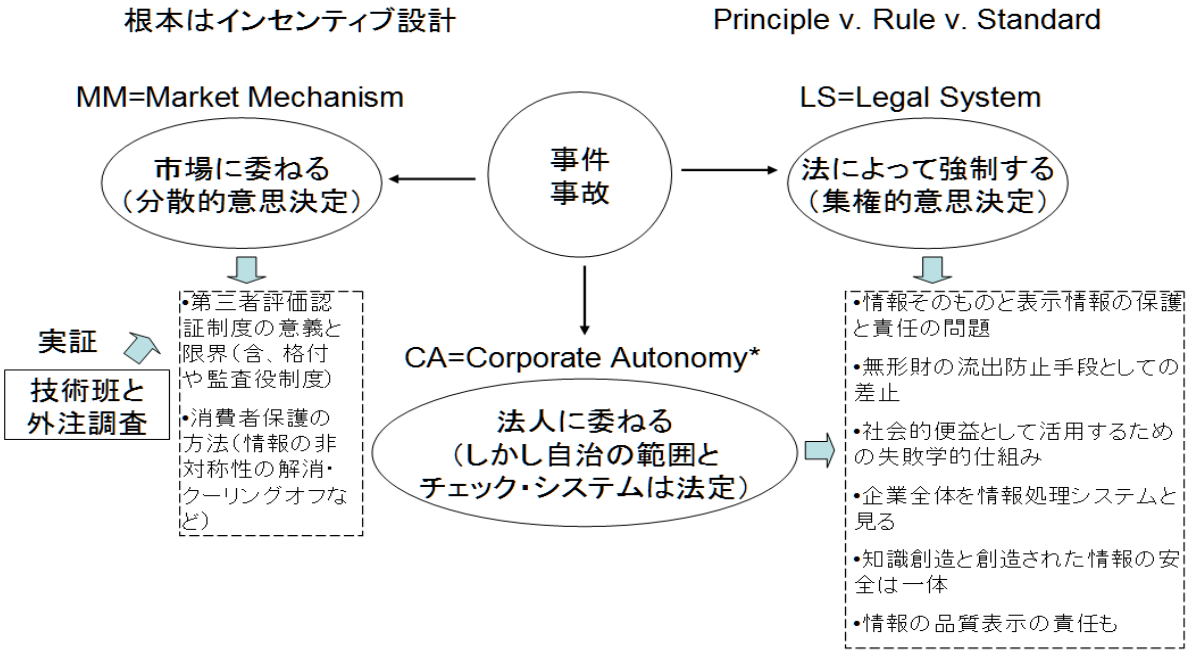
これを元に、責任のあり方を正負のサンクション（ペナルティが課される場合のほか、報奨金が得られる場合を含む）として分類した結果、次図のようなパターンを抽出した。（Ⅰ）が従来の責任のあり方だが、情報セキュリティについては、（Ⅱ）（Ⅲ）（Ⅳ）のほか、法人に特有な責任のあり方も論議せざるを得ないことが判明した。

責任の分類（正負の Sanction として）



第 3 は、ガバナンス制度の類型化である。上記を踏まえ、「法学」「経済学」「経営学」の社会科学の 3 分野の理論を下敷きにして、以下のような多角的検討を行った。この結果を、社会全体が共有するとともに、ブレイクダウンした「提言」として訴求するに至った。

また、一部は当大学院の科目に組み込み、知識レベルを上げると共に、社会的な認知度の向上をも目指したい。



*この仕組みの有効性とその適用範囲を見つけることが、corporate governanceの問題であり、その情報セキュリティ版が本研究のテーマ

第 3 で述べた具体的な提言項目は、以下のとおりである。

ガバナンスのあり方として

・外部委託と情報セキュリティ対策に関する提言(佐藤執筆)
・アジア地域に進出している日本企業の情報セキュリティマネジメントの現状と取組みの改善(早貸執筆)
・情報セキュリティ・ガバナンスにおける内部統制規制のあり方(柿崎執筆)

シグナル情報のあり方として

・第三者認証制度に求められる８原則(鈴木執筆)
・「見えないものの品質保証」に関する提言(林・田川執筆)
・表示に伴う責任論(林・田川執筆)

情報と情報セキュリティの一般論として

・企業における情報セキュリティの強化に貢献する法制度の実現に関する提言(鈴木・湯淺執筆)
・情報法の客体としての「情報」の捉え方に関する提言(林執筆)
・情報漏洩と個人データの保護に関する提言(林執筆)

３．研究開発構想

研究開発開始時点での研究開発構想は、次のような内容であった。

「情報セキュリティに関するインシデントの類型別に、誰がどのような責任を負うべきか、あるいは責任の追及よりも今後の改善策の検討により多くの資源を投入すべきか等について、判断基準を提供する。また判断基準が提供できないケースについては、その原因を明確にする。」

2 年半の研究開発の当初は、企業活動や社会生活において、情報というものが決定的役割を果たすようになったことを踏まえ、「法」及び「経営管理」に「技術」の視点を加えた形で、情報セキュリティガバナンスのあり方を検討することを目的としていた。班構成は、法制度班、経営管理班、技術班に加え、全体の取りまとめ行う総括班の 4 班体制でスタートした。

既に述べたとおり、研究開発は、法制度班、経営管理班の定期会合、技術班へのフィードバック、定期的なシンポジウムやワークショップの開催、出張やヒアリング等を通じて進めており、概ね、開発計画に沿った態様であったと考えている。2009 年度に最終報告書起草グループを構成して取りまとめに入った点についても同様である。

また、2008 年度からは、富士通総研及び技術班における実証調査が行われた。これは、当初は予定していなかったが、研究を進めていく中で情報セキュリティガバナンスを実効化するための裏付調査の必要性を実感し、実施したものである。

研究内容に関して、研究開発活動の途中までは、法制度班は個人情報保護法を中心とし、経営管理班は ISMS 制度を中心とするなどのばらつきが見られたが、各班の報告書を取りまとめる段階で、論点を集約することができた。具体的な研究成果は 4 を参照されたい。

その結果、最終的な研究開発目標は以下のように修正された。構想に大きな変更はないが、当初よりも具体化した目標となっている。

「日々膨大な情報を取り扱いリスク･テイカーである企業を対象に、情報セキュリティを実効あらしめるために、いかなる「制度」が望ましいかという視点から、そのガバナンスのあり方を検討する。リスク類型別のケース・スタディにより、消費者の視点に立って問題点を摘出する。そして、誰がどのような責任を負うべきか、あるいは責任の追及よりも今後の改善策の検討により多くの資源を投入すべきか等について、判断基準を提供する。また判断基準が提供できないケースについては、その原因を明確にする。」

かかる研究開発構想のために各グループが担った役割は、以下のとおりである。

総括班：研究グループ全体のとりまとめを行う。

法制度班：「情報」と「安全」に関する法制度のあり方を検討し、情報セキュリティガバナンスを実効あらしめるためにはいかなる法制度が望ましいかについて、責任論を中心に検討する。

経営管理班：経営学的観点から、第三者認証制度のあり方を中心に、情報セキュリティガバナンスの実効化を検討する。その際、内部統制、監査論から得られる知見等を参考にするほか、実

証調査も行う。

技術班：法制度班、経営管理班からのフィードバックを受け、情報セキュリティガバナンスと技術の関わりについて検討する。企業における情報の流れを把握するための実証調査を行う。

最終報告書起草グループ：法制度班、経営管理班、技術班の検討結果を踏まえ、最終報告書を起草する。

その後の展開から生まれた新たな目標ないし課題は、最終報告書の中の個別提言を参照されたい。

４．研究開発成果

この項目については、以下の構成により報告する。

第１編　総論編
1　課題の設定から仮説の定立に至るまで
2　背景となる理論的研究
3　実証研究（詳細は「第３編　実証研究編」参照）
4　経営層に向けた提言
5　個別提言
第２編　理論研究編
1　情報セキュリティとガバナンス
2　情報セキュリティガバナンスにおける表示と法的責任
3　第三者評価認証制度
4　プライバシーマーク制度とその問題点
5　ISMS 適合性評価制度とその問題点～外部委託を中心に
付論１　国家における情報ガバナンス(別添)
付論２　情報マネジメントポリシーに関する証跡確保と従業員のプライバシーの相剋
(別添)
第３編　実証研究編
1　富士通総研調査「情報セキュリティのガバナンスと逸脱行動に関する調査」
2　技術班調査「ネットワークの情報流通と企業ガバナンスに関する調査」
第４編　個別提言
1　ガバナンスのあり方に関する提言
・外部委託と情報セキュリティ対策に関する提言(佐藤執筆)
・アジア地域に進出している日本企業の情報セキュリティマネジメントの現状と取組みの改善(早貸執筆)
・情報セキュリティ・ガバナンスにおける内部統制規制のあり方(柿崎執筆)
2　シグナル情報のあり方に関する提言
・第三者認証制度に求められる８原則(鈴木執筆)
・「見えないものの品質保証」に関する提言(林・田川執筆)
・表示に伴う責任論(林・田川執筆)
3　情報と情報セキュリティの一般論に関する提言
・企業における情報セキュリティの強化に貢献する法制度の実現に関する提言(鈴木・湯淺執筆)
・情報法の客体としての「情報」の捉え方に関する提言(林執筆)
・情報漏洩と個人データの保護に関する提言(林執筆)

第 1 編　総論編

1　課題の設定から仮説の定立に至るまで

本プロジェクトの課題の設定から仮説の定立に至る検討過程で、以下のような事項について検討を行い、知見を得た。

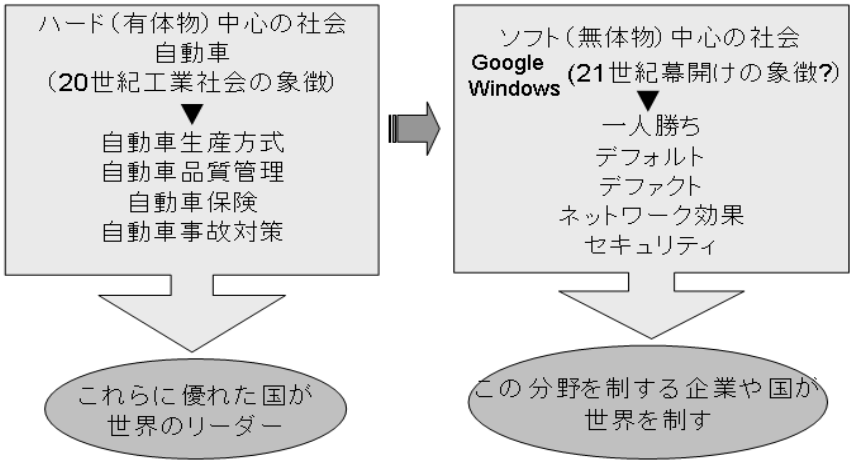
1.1 情報セキュリティの発展に関する時代区分

コンピュータやネットワークの発展に伴い、情報セキュリティの対象範囲が拡大しているが、本プロジェクトでは、コンピュータおよびネットワークの発展に着目して、情報セキュリティの発展段階を以下の４段階に区分した。

1)スタンドアローン時代（～1950 年代）
　暗号研究家やコンピュータ専門家によるセキュリティ
2)メインフレーム・オンライン時代（1960 年代～1970 年代）
　コンピュータを中心にしたシステム・セキュリティ
3）パソコンとインターネット時代（1980 年代～2000 年代前半）
　上記に加えて、ネットワークに係るウイルス・ワーム、BOT、システム対する攻撃、ネット詐欺、ソーシャル・エンジニアリングなどに対する防御、電子認証・電子マネーなどの新しいアプリケーションに関するセキュリティ
4）クラウド・コンピューティング時代（2000 年代後半～）
　情報の共有と囲い込み、ID による追跡可能性とプライバシーなどトレードオフの増大、両用技術（軍事・民生に加え、民生内でのトレードオフ）の発展の下でのセキュリティ

1.2 情報セキュリティの社会的意義づけ

情報セキュリティの社会的意義に関して、有体物中心から無体物中心の社会へ移行する大きな流れに着目して、意義づけを行った。



1.3 リスク類型別のケース・スタディ

個人情報保護およびスパムメール問題を取り上げて検討を行い、以下の知見を得た。

1.3.1 個人情報保護対策と仕事の効率的遂行のバランス

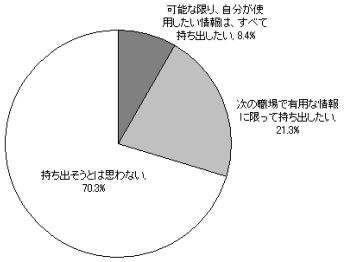
個人情報保護対策として、私有パソコンの接続禁止.外部メモリの使用禁止．メモリなしパソコン（thin client)導入などハードウェア管理の厳格化が見られ、また、入退室管理、モニタリング、ログの保存、教育・訓練、社員からの確認書提出、契約相手との違約金の予定など業務運営上の対策も行われている。

このような個人情報保護対策の厳格な実行が仕事の効率的かつ創造的な遂行に関して悪影響を与えていないのか調査する必要性があると考え、「やらされ」感や、生産性との関係を何らかの形で定量化するため、富士通総研アンケート調査を実施した。

（調査結果等については、3.において要旨を、また、詳細については、第３編　実証調査編を参照）

1.3.2 トレンドマイクロ社の意識調査結果

職場における機密情報の持ち出しの可能性についてトレンドマイクロ社がアンケート調査を行っている。2009 年 11 月 11 日に公表されたトレンドマイクロ社の「業務情報の取り扱いに関する調査結果」によれば、転職や異動時に業務情報も持っていきたいという回答者が半数を超えたほか、機密情報の持ち出しは 80%以上が特定、把握されないと考えているようだ。



また、回答者の多くが勤め先の機密情報を持ち出せるとの認識を有しているようである。勤務先で業務上の機密情報が漏れないように守られているかという質問には、「守られていない（漏れているかもしれない)」が 12.3%、「守ろうとしているが、実効性に欠けている（やろうと思えば持ち出せてしまう)」が 55.6%、「しっかりと守られている（絶対に漏れないようになっている)」が 32.0%だった。

加えて、回答者の 85.7%が自社の機密情報を無断で持ち出したとしても、情報の持ち出しを把握できないか、第三者から通報されたり情報漏洩事件として発覚しなければ特定されないと考えているという。この調査結果は、種々の対策にも関わらず、機密情報の社外流出のリスクはかなり高いことが示唆しているように考えられる。

1.3.3 個人情報漏えい時の事象

個人情報の法的保護の難しさに関して、個人対法人、秘匿対公開、権利付与対事後救済の視点からどのような難しさがあるかおよび二次被害の予測しにくさについて検討した。(1.3.4 項参照)
また、帰責（責任の配分）の難しさに関しては、個人対法人、行政責任対司法責任、責任の希釈化対厳罰化、責任と免責、保険などの視点から分析した。

実際の情報漏えい時においては、リスク評価よりもマスメディア対応に重点が置かれ、かつ、マスメディアの報道も実害よりも安全管理義務違反に着目した報道が中心になっている事象が見られる。

1.3.4 個人情報の法的保護の難しさ

以下の概念枠組みによって、個人情報保護の法的な難しさを捉えた。

	公開情報	非公開(秘匿)情報
法人等に帰属する情報	特許発明	営業秘密に係る情報 通信の秘密に係る情報
	著作物	
個人に帰属する情報	個人情報*	営業秘密に係る情報 通信の秘密に係る情報 プライバシーに係る情報
	特許発明	

＊個人情報は①人格権と財産権を切り離しにくい．②事前の権利設定が難しい．
③2次、3次被害者が予見不可能．④リスクの受容水準が自分で決められないため、従来のマネジメント手法が使えない．

1.3.5 スパムメール

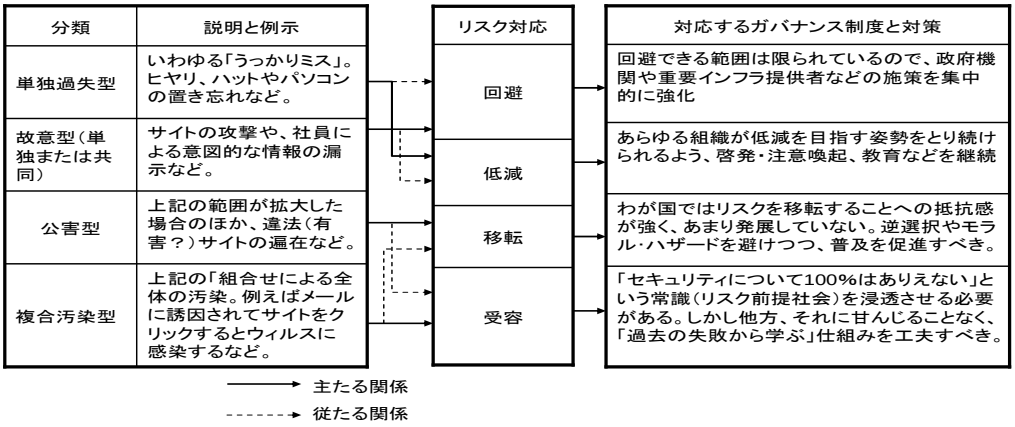
以下の事項について、多面的な対策・責任論の視点から検討を行った。

・表現の自由・営業の自由対受信者や社会の迷惑
・迷惑メール防止法の意義と限界

・情報仲介者への期待と通信の秘密との関連
・技術・法・経営管理・倫理・啓発を総動員
・消費者保護の視点の必要性（米国の FTC）
・ワクチン開発者の bounty を与えるなどの、プラスのサンクション
・事故調査的な機能強化、司法取引の導入
（独禁法で予想以上の成果を挙げているリニエンシー制度を参考に）
・国際共助の不可欠性

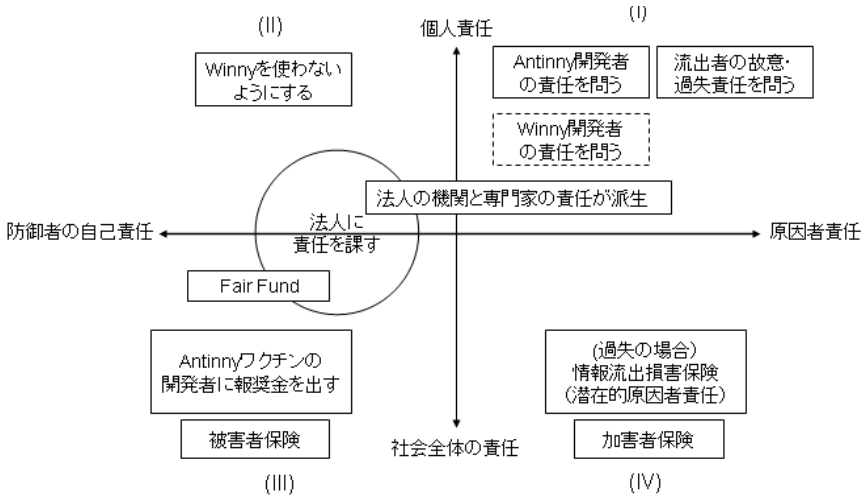
1.3.6 インシデントの分類とリスク対応とガバナンス制度のあり方

研究開発目標を達成するために、上記に述べた個人情報漏えいやスパムメールなどのインシデントを分析し、リスク対応やガバナンス制度との間に、次表のような対応関係があることを解明した。



これを元に、責任のあり方を正負のサンクション（ペナルティが課される場合のほか、報奨金が得られる場合を含む）として分類した結果、次図のようなパターンを抽出した。（Ⅰ）が従来の責任のあり方であるが、情報セキュリティについては、（Ⅱ）（Ⅲ）（Ⅳ）のほか、法人に特有な責任のあり方も論議せざるを得ないことが判明した。

責任の分類（正負の Sanction として）



2　背景となる理論的研究

前１の事項に関する検討を深めるため、その背景となる理論的研究として、以下の事項に関して検討を行い、それぞれについて知見を得た。

2.1 情報セキュリティの保護対象である「情報資産」の再定義

以下のような考え方に基づき「情報資産」の再定義を行った。
・従来の「情報資産」という概念を、ストックとしての「情報資産」のほか、フローとしての「情報の流通制御」を含むものと捉えなおす。

・「情報資産」には、「公開して守る」知的財産（主として integrity）と「秘匿して守る」秘密（confidentiality）との両方がある。
・従来「情報資産」に入っていなかった「シグナル情報」（それ自体には資産価値はないが、「製品・サービス」の流通を円滑にするために不可欠な、品質などの判断用材料）の存在を認め、その位置づけ明確にする。
・情報セキュリティガバナンスに関して、静態的ガバナンスから動態的ガバナンスへとガバナンスのスコープを拡大することで、より実効性のある情報セキュリティガバナンスが実現するのはないか。

2.2 流通制御（動態的ガバナンス）の必要性と方法

2.1 の動態的ガバナンスの必要性と方法について、以下のように考え方を整理した。
・企業活動の多層化・重畳化に伴い、情報の移転によって価値が生ずる（バリュー・チェーン）
・情報仲介者の役割の増大
・「製品・サービス」の流通を取引するためには価格情報だけでは不十分で、何らかの品質情報が不可欠

⇩

・企業間　　情報流通の実態調査の必要
・品質表示情報の不可欠性については、度重なる偽装事件（耐震強度、賞味・消費期限、原産地、財務諸表 etc）で明らか

2.3 情報セキュリティに関する法人責任論

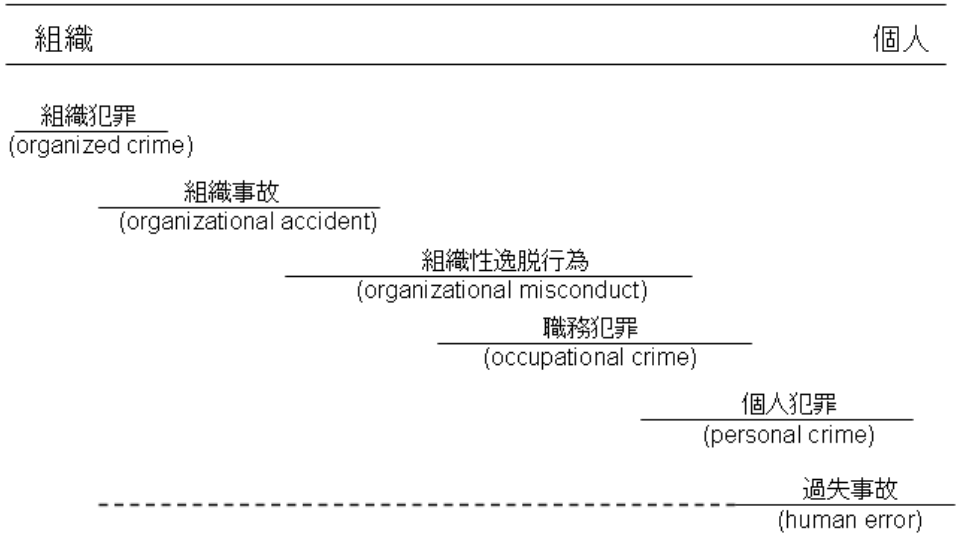
2.3.1 なぜ法人の責任を問うのか

情報セキュリティにおいて、法人責任が重要な検討事項になる理由について整理した。
・法人は、情報量、伝達速度、イノベーションなどの面で巨大な情報処理装置であり、現代の情報蓄積および流通に大きなウエイトを有している。
・存在感、規模、社会的責任（不祥事）などの面においても大きな社会的存在である。
・業務処理のスピードが速く、変化にも対応が早く、かつ、しがらみが少ないので、官よりもダイナミックな行動を取り得る。一方で、逸脱行動もダイナミックになり得る。
・法人は個人を包摂しており、個人を上回る規律（企業風土）のもとで社会的な活動を行っているが、ときとして、個人的逸脱行為だけではなく会社ぐるみと言われるような組織性逸脱が見られる。
・研究計画目標の項で述べたように、法人の基本的な特徴はリスク・テーカーであることであり、リスク管理の主体である。また、法人は他の主体よりも低コストでリスク・テークできる LCRT(Least Cost Risk Taker)。このリスク・テーカーである法人が日々膨大な情報を取り扱っており、法人における情報セキュリティを実効あらしめるためにはいかなるガバナンスが望ましいかを考える必要がある。
・法人においては、エージェンシー問題などステークホルダー（あるいは利害関係者）間の利害不一致が例外的事象ではなく、ガバナンス上の困難性を有している。このガバナンスの困難性は、情報セキュリティ分野においても例外ではない。

2.3.2 法人責任に関する検討対象と課題

さしむき民事責任を中心に「表示と責任」の問題の検討に着手する。法人に対する政処分に関しては、複雑な事象に対応するには行政罰（行政処分）が向いているとの説（白石［2007］）もあるが、権力が信頼できるかどうかの問題が残る。一方、法人の刑事的責任に関しては、両罰規定を経由せず、法人の犯罪能力を認めるべきだとする一般論（甲斐(編)［2008］、樋口［200６］）と、企業にも保護観察処分等が必要だとする政策論（川崎［2004］）などがある。

また、法人責任を問う際の、法人の行為類型として、組織の行為として捉えられるべき行為と個人の行為として捉えられるべき行為の類型化を行った。



2.4 見えないものの品質保証

前述したように情報資産の再定義を行い、情報資産としてシグナル情報も含めることとした。その場合、より広汎な「見えないものの品質保証」の問題の検討が必要になる。そこで、表示と責任の問題を含めて検討を行い、以下の知見を得た。

2.4.1「見えないものの品質保証」について得られた基本的な知見

・サービスや情報などの財は、見たり触ったりして品質を確認することができないので、価格さえ分かれば取引可能ということにはならない。
・売り手と買い手に「情報の非対称性」があると、市場は機能しない。（レモンの市場、逆選択）また、保険も、モラル・ハザードなどの落とし穴がある。
・したがって、価格のほかに「品質表示情報」を提供し、その情報の信頼を維持する必要がある。
・提供方法としては、自己確認、第三者認証、格付け、検査・検収などがあり、補助手段として資格制度などがある。
・これらは、JAS 法が典型的であるが、何らかの「表示制度」と結び付いていることが多い。

2.4.2 情報の非対称性を軽減する対策

一般的には次のようなものが考えられていることを確認した。

・シグナリング
　商品の品質に関する情報（シグナル）を買い手に提示しなければならないようにし、情報の格差を縮小する。例えば中古自動車の場合、自動車の年式や走行距離、修理記録などを開示しなければならない法律を制定するなど
・自己選択
　買い手に関する情報を、買い手自身の選択を通して提示させる。例えば自動車保険会社が走行距離に応じた複数の割引保険を用意し、どの保険を選択するかを決定させる方法。これによって保険会社は、加入者の自動車利用頻度を確認できる
・スクリーニング
　入学試験や入社試験、資格試験などを行ない、商品の品質を保証する。例えば労働市場において企業が労働者を雇用しようとする場合、労働者に対して入社試験を課すなど
・第三者認証
　信頼できる第三者に品質を審査させ信頼度を高める

2.4.3 上記の表示に伴う責任問題

以下の知見を得た。

・表示を偽ったり、表示と違った結果を収束したときの責任は、詐欺（刑法 246 条）、優良・誤認表示（景表法 4 条）、表示の混同等（不正競争防止法 2 条 1～3 号）などで責任を追及され得るが、よほどの場合に限られている。
・表示がマークなどの形で提供され、その掲出資格が法的にあるいは契約上で明確にされている

場合は、マークのはく奪があり得るが、発動されるのはごく稀。
・表示違反の差止請求の例は寡聞にして聞かない。
・表示違反の不法行為責任を問うた例も少ないと思われる。
・表示と契約責任については、藤田[1994]による詳細な分析がある。
・商標法、JAS 法、経済学における「レモン市場理論」などを総合する必要がある。

2.4.4 契約法における表示と責任

日本においては、表示と契約責任については、藤田[1994]による詳細な分析がある。
また、イギリスにおけるケースとしては、以下の知見がある。

「物品の売買契約についての法は、黙示的条項に従って、物品の品質自体の水準にかかわる履行水準を定めるものである。他方ある契約が役務提供契約であるとされた場合には、コモンロー上の原則によると、役務の提供者は、合理的な注意と技能をもって役務を提供することが義務づけられ、履行の過程にかわる義務のみが課され、提供される目的物の品質自体にかかわる黙示的条項は存在しない。」

出典：川和功子「英国法における電子情報取引契約をめぐる契約法上の表示責任（上）（下）」NBL、2007年1月号、2月号

さらに、第三者認証機関が行った認証行為の責任について、トラストマーク組織（TMOs：Trustmark Organisations）を例にした以下の知見も得られた。

「不正確なトラストマークを信頼して、損害を被った電子商取引を行った消費者に対して、TMOs の損害賠償責任（liability）はあるのか？　理論的に言えば、第三者たる TMOs の責任を問う十分な法的な根拠はある。しかしながら、実際的には、TMOs が免責される可能性の方が高い。このため、現時点では、ヨーロッパにおいては、電子商取引を行った消費者に対する TMOs の法的責任は事実上存在しないと言えよう。」

出典：Paolo Balboni[2009]“Trustmarks in E-Commerce: the Value of Web Seals and the Liability of their Providers”

2.4.5 コミットメント責任

コミットメント責任を定義するとともに、その責任がどのような場合に発生するかについて知見を得た。

・定義：事業者が、情報管理を含む経営管理に関する約束事を利害関係者に対して、表示または情報開示したにも関わらず、それに違反することによって生じる責任（法的責任を中心としながらも、より広い概念としての sanction。SLA=Service Level Agreement に記載されれば契約責任になる）
・責任が発生する場合
  1） 自己確認の場合
  2） 第三者評価認証制度による場合
  3） 個別法の規定による場合
  4） （上記いずれについても）検査・検定機関が関係する場合
  5） （上記いずれについても）資格制度と専門家が関係する場合

2.5 ガバナンスの現状とあり方

主として、内部統制に着眼して、ガバナンスの現状とあり方ついて検討した。

2.5.1 財務諸表監査と内部統制監査との関係の捉え方

これに関して、早稲田大学 GCOE プログラムの研究成果から、以下の知見を得た。

財務諸表監査との関係 / 監査の主題との関係	財務諸表監査の枠組みの中		財務諸表監査の枠組みの外
	財務諸表の適正表示の枠組みの中	財務諸表の適正表示の枠組みの外	
言明の監査として設計	I	III(日本) (2007年1月1日現在のアメリカ)	V
非言明の監査として設計	II	IV (2008年1月1日現在のアメリカ)	VI

出典： 鳥羽至英「財務諸表監査と内部統制監査を一体的に運営する意味について」
『2009年早稲田大学公開シンポジウム資料』(2009.12.17)を一部修正。なお、鳥羽説はIII

2.5.2 内部統制の経営者評価と監査意見

これに関して、早稲田大学 GCOE プログラムの研究成果（2009 年 3 月決算会社の集計）から、以下の知見を得た。

経営者評価 \ 内部統制監査意見	無限定適正	意見不表明	非監査(注)	合計
内部統制は有効	2,603		2	2,605
重要な欠陥があり内部統制は有効でない	55	1		56
内部統制の評価結果を表明できない		9		9
合計	2,658	10	2	2,670

(注)上場会社以外の有価証券報告書提出会社は内部統制報告書を任意提出できる、17社が任意提出したが、このうち2社については内部統制監査意見の添付がなかったことによる

最終的に経営者と監査人の見解の大きな相違は見られなかった

出典:山田善隆「内部統制監査実施初年度の状況と今後の課題」『2009年度早稲田大学公開シンポジウム資料』(2009.12.17)を一部修正

2.5.3 内部統制報告書における重大な欠陥の扱い

これに関して、早稲田大学 GCOE プログラムの研究成果から、以下の知見を得た。

分類	社数	割合(%)
重要な欠陥の存在が財務諸表の重要な修正等として顕在化したことによる(注)	54	96.4
財務諸表の重要な修正等には至っていないが、潜在的可能性が識別されたことによる	0	0.0
リスクの評価と対応の未実施/未完了	2	3.6
合計	56	100.0

(注)財務諸表の公表前に監査人による財務諸表監査の過程で修正されたものを含む
※上記の分類は、内部統制報告書または独立監査人による監査報告書に顕在化した事象の存在を示す記載があるかどうかによった

財務報告における不正や誤謬の潜在的な可能性よりも顕在化した事実をもって重要な欠陥ありとするケースがほとんどであった。

出典:山田善隆「内部統制監査実施初年度の状況と今後の課題」『2009年度早稲田大学公開シンポジウム資料』(2009.12.17)を一部修正

2.5.4 監査人の対応に関してよく聞かれる批判

主たる批判は、以下の通りである。

・過度に保守的な判断がなされている。

・画一的な対応がなされている。
・様々な文書化が求められる。

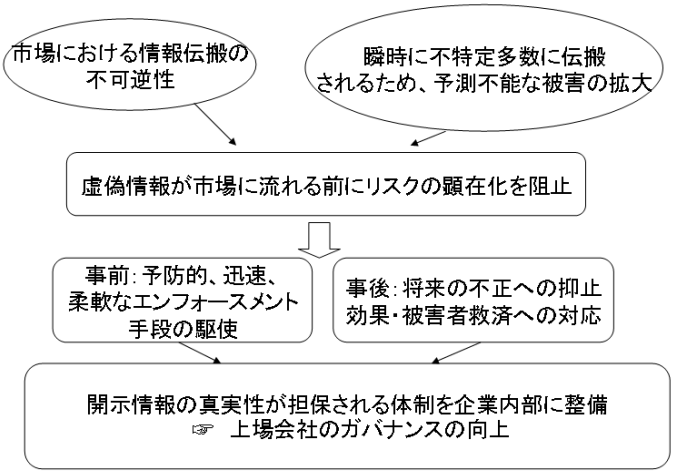
⇩

内部統制監査に　　おいては、特に従来の財務諸表監査とは性質が異なる要素について、監査人により高度な対応を求めるものであったが、その対応にばらつきが見られた。

出典：山田善隆「内部統制監査実施初年度の状況と今後の課題」『2009 年度早稲田大学公開シンポジウム資料』（2009.12.17）を一部修正

2.5.5 市場法における内部統制規制の枠組み

この枠組みに関して、柿崎の研究から、以下の知見を得た。



出典：柿崎環[2009]「米国におけるSOX法内部統制の現状と課題」『2009年度早稲田大学公開シンポジウム資料』(2009.12.17)

2.5.6 ガバナンスのあり方を考える上でのひとつの指摘

規律を守る一方で、のびのびと個性を発揮する必要性を指摘する以下の声があるが
これは、3. 実証研究 3.1「セキュリティの実効性と企業風土に関する調査」に関する実証調査と、同じ問題意識に立つものである。

企業の規範を遵守しながら、協奏曲におけるカデンツァのように内容ある華やかな舞を舞いまくる！これが私の心からの切なる願いです。最近はCSRとかコンプライアンスという美名の下に法律遵守やcheck and controlということが強調され、のびのびと個性が発揮されていないのは非常に残念なことだと思います。このエンパワーメントとカデンツァは、相互連関性があり、是非リーダーとしてそれを奨励して欲しいと思います。

出典：渡邊五郎氏（元三井化学会長、元三井物産副社長）の一柳塾における講演（2009.7.10）

2.5.7 格付会社の法的規制（2009 年金商法改正）に見る 2 次情報の保護と表示責任

このことに関して、以下の知見を得た。

・IOSCO*の基本行動規範をベースに 4 つの柱に集約
1)誠実義務：信用格付業者は、独立した立場において公正かつ誠実にその業務を遂行しなければならない（66 条の 32）
2)情報開示義務：適時又は定期的な情報開示が必要（66 条の 36、66 条の 39 など）
3)体制整備義務：業務の品質管理、利益相反防止その他業務の執行の適正を確保するための措置を含む業務管理体制を整備しなければならない(66 条の 30)
4)禁止行為：特定の行為（密接な関係を有するものへの格付の提供）が禁止される（66 条の 35）
*International Organization for Securities Commissioners and Similar Agencies

2.5.8 米国の SEC（証券取引委員会）の段階的エンフォースメントの仕組み

ガバナンスの類型として、米国の SEC（証券取引委員会）が企業に対して行っている、段階的エンフォースメントの仕組みについて知見を得た。この仕組みは、SEC の証券市場機能の公正性確保に向けた事前の予防的法執行と、事後の厳格な法執行の両面のアプローチを取っていることが特徴である。

・第 1 段階：非公式の準備調査段階では、SEC は問題情報を公表せず、調査対象企業の経営者、

内部監査人、法務部長らと面談し、企業内部で早期に問題の解決と是正措置の導入を迫ることにより、正式な法執行手続き段階に移行しないまま対処する手法がとられている。

・第 2 段階：おもに会計上の問題などの発覚を契機として、企業の Form8-K（臨時報告書)、Form10-Q(四半期報告書)、Form10-K(年次報告書)等の開示事項につき、SEC から staff comment letter を送付して、詳細な説明と場合によっては restatement を企業に要求する。

・第 3 段階：企業から応答書簡(response letter)なり、各開示文書の restatement を SEC に提出。

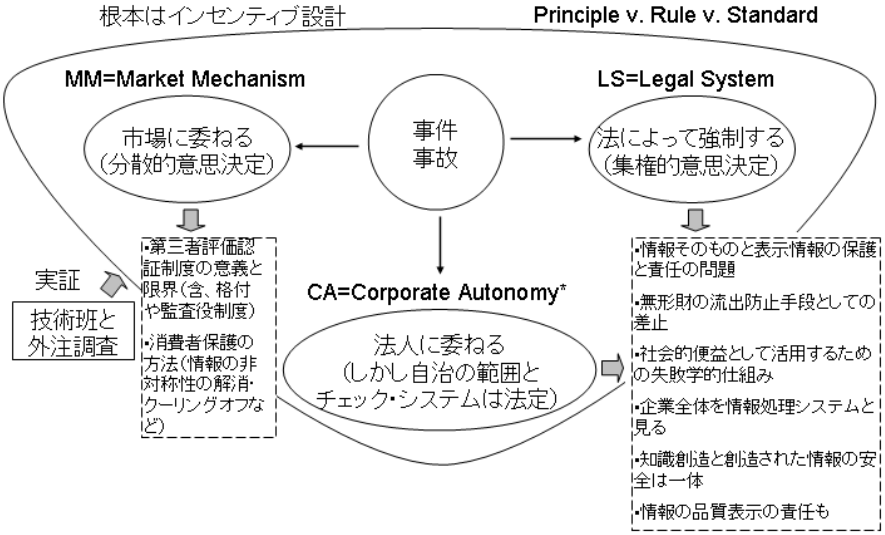
・第 4 段階：正式なエンフォースメント段階：litigation releases の発行、排除措置命令、民事制裁金、利益の吐き出し、取締役・役員の就業禁止等。悪質な場合には、Rule10(b)-5 の適用、司法省による刑事訴追へ

出典： 柿崎環[2009]「米国におけるSOX法内部統制の現状と課題」『2009年度早稲田大学公開シンポジウム資料』(2009.12.17)

2.6 ガバナンスの類型化

「法学」「経済学」「経営学」の社会科学の 3 分野の理論を下敷きにして、以下のような多角的検討を行った。この結果を、社会全体が共有するとともに、ブレイクダウンした「提言」として訴求するに至った。

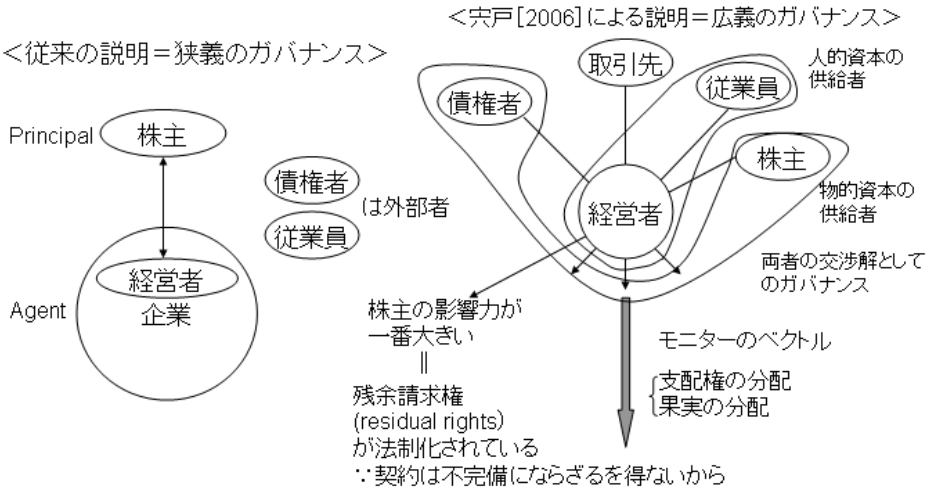
また、一部は当大学院の科目に組み込み、知識レベルを上げると共に、社会的な認知度の向上をも目指したい。



*この仕組みの有効性とその適用範囲を見つけることが、corporate governanceの問題であり、
その情報セキュリティ版が本研究のテーマ

2.7 コーポレートガバナンスに関する新しい視点

コーポレートガバナンスをインセンティブ設計の視点から捉えると、従来のガバナンス概念ではなく、広義のガバナンス概念が情報セキュリティガバナンスにとっても示唆に富むとの知見を得た。



出典：宍戸善一[2006]『動機付けの仕組としての企業』有斐閣

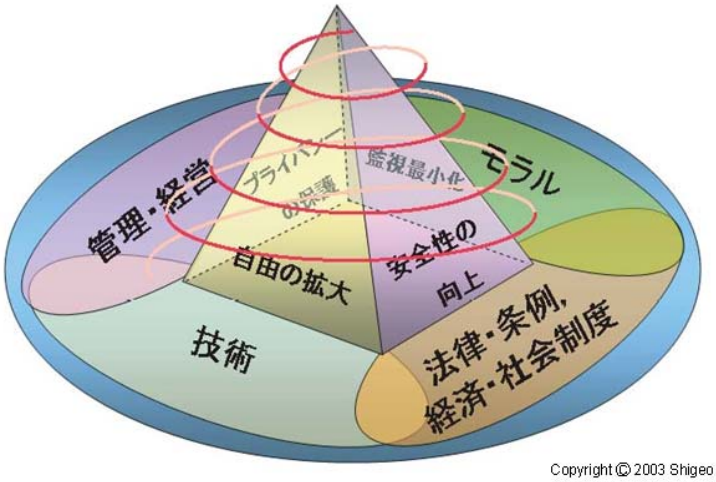
2.8 情報セキュリティ研究の基礎的課題

情報セキュリティ研究の基礎的課題として、情報法」の客体論を以下のように整理した。
情報法という法体系で守ろうとする「客体=情報」とは何か？ どのような「情報」が保護され、どのようなものが禁止されるのか？ ディジタル化すればビット列に他ならない「客体」の差はどこから来るのか？

	客体	具体例
保護	一次情報	知的財産、秘密、個人情報*
	二次情報	メタ情報（属性情報）、品質表示情報、検索結果？
禁止	時と場所と状態による	いわゆる有害情報
	いかなる場合にも	違法情報、ウィルス

＊アメリカの著作権制度のように人格権部分を切り離すことが前提

また、情報セキュリティ研究の到達点としての総合科学化の枠組みについては、情報セキュリティ大学院大学建学以来、一貫して追求してきたものである。技術的課題についてはそれなりの研究の蓄積と交流がなされているが、社会・人文科学の課題については、学際的アプローチが乏しく、方法論を模索している状態であった。本件研究を実施することにより、少なくとも方法論については一定の知見を得た。



3　実証研究（詳細は「第 3 編　実証研究編」参照）

実証研究として、以下の 4 つの調査を行った。

3.1 セキュリティの実効性と企業風土に関する調査

調査方法等は以下の通り。

- 目的　企業におけるセキュリティ・ポリシーの有効性は、組織風土や社員意識と、どのような係りを持っているのかを、知りたい。
- 時期　１回目＝２００８年秋、２回目＝２００９年秋
- 方法　インターネット調査会社によるウエブ調査
- サンプル数　１回目＝１，７００、 ２回目＝２，０００
- 委託先　富士通総研

調査結果として以下の知見を得た。

- まずは、ルールの整備が必要。
- 職場の実態を無視して、ルールを過度に厳格に適用すると、ルールが機能せず、逸脱行動も阻止できず、むしろ逆効果。
- 個人レベルで見れば、セキュリティの知識が高いほど逸脱が少ない、とは言えない。
- セキュリティ担当者と利用者間の、十分な話し合いと相互理解、利用者からの提言などが効果的。
- ルール制定後の、トップからボトムを巻き込んだ運用のあり方が重要。

3.2 会社の情報流通実態調査

調査方法等は以下の通り。

- 目的　企業内、グループ会社内、外部企業や顧客との間など、情報はどのように流れているのか、定量的に知りたい。
- 対象　ベンチャー企業Ｊ 社と中堅企業Ｉ 社
- 時期　前者＝２００８年秋、後者＝２００９年秋
- 方法　情報技研㈱開発によるログ分析ソフトによる

調査結果として以下の知見を得た。

- ポリシーが緩やかなＪ 社と、文面上は厳し目のＩ 社の間で、利用形態（ウエブへのアクセス等）に有意差は見られなかった。
- しかし両社とも、社員の自制心が効いているのか、会社業務に悪影響を及ぼすような利用例は見られなかった。
- セキュリティ施策の実効性を判断するには、ポリシーやマニュアルを見ていただけではダメで、実態に踏み込まなければならない。

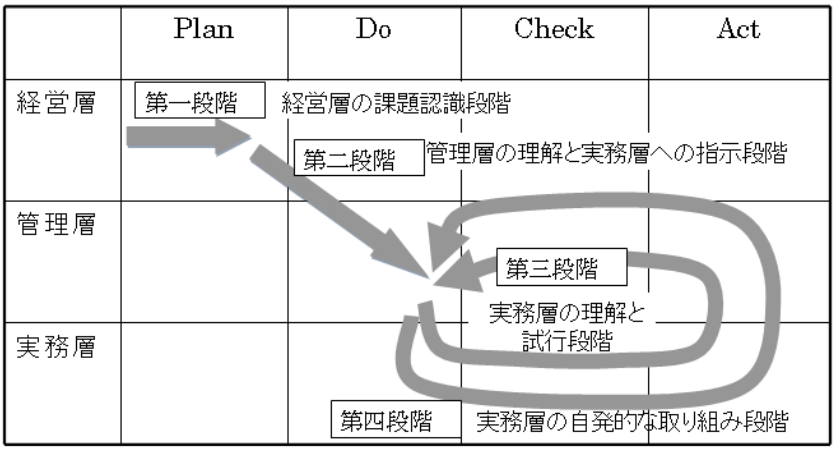
3.3　IISEC における P マーク取得企業調査

調査方法等は以下の通り。

- 目的　P マーク取得企業は、3 年後の更新時に当初の対策とレベルを維持しているか、を知りたい。
- 方法　ヒアリング調査
- 対象　日本データ通信協会からの P マーク取得企業のうち、管理レベルの高いと思われる 11 社（資本金の平均＝7 億円、売上高の平均＝100 億円）

調査結果として以下の知見を得た。

- P マーク取得企業において、個人情報保護対策に関する効果的な PDCA を回すためには、トップの役割が重要であり、とりわけ、第 4 段階の取り組みが行われることが効果的であるとの知見を得た。



出典：猪野・松田・板倉[2010]「情報漏えい対策における持続可能なPDCAサイクルを推進する方法」JSCIS発表予定資料

3.4 CIO(CISO を含む) 調査

調査方法等は以下の通り。

- 目的　アメリカにおける CIO(CISO を含む) とは、どのようなバックグラウンドを持つ人か、またどのような教育を受けているか、を知りたい。
- 時期　2009 年 11 月
- 方法　訪問調査

調査結果として以下の知見を得た。

- CIO には技術系出身とビジネス・スクール出身者がいる。
- 前者は各種の資格取得で、後者は MBA コースなどで育てられている。
- 政府助成の仕組みがある。
- CEO や CFO ほどに地位が固まっていない（制度化されていない）。

4　経営層に向けた提言

4.1 社会的アピールと情報セキュリティ文化の醸成の関する提言

企業経営における情報セキュリティの重要性に関して、トップ・エグゼクティブ（特に文系出身者）が、以下 5 項目の認識を共有すべきであるという結論に到達した。これら 5 項目は、本研究から生まれる諸提言を理解していただくための、基礎となるとともに、わが国固有の情報セキュリティ文化の醸成に寄与するものである。

認識１．(リスク･テーカーとしての企業)
企業はリスク・テーカーであり、リスクを低減したり、ヘッジしたり、移転したりすることは出来るが、それをゼロにすることはできない。

認識２．(業務のシステム依存)
企業活動の大部分は、コンピュータとネットワーク・システムに支えられており、そのリスク対策が情報セキュリティであるから、これは経営の根幹に触れる問題である。

認識３．(経営者自身に課せられた最適化問題)
情報セキュリティがリスク対策である以上、それは全社的に費用対効果を最適化すべきものであり、他の経営意思決定と何ら異なるものではない（専門家に任せておいて済むものではない)。

認識４．(ガバナンス制度間の整合性)
情報セキュリティ対策は、経営全般のガバナンスと責任のあり方（内部統制、コンプライアンス、品質管理、環境適応、企業の社会的責任）などと整合的、かつ統制の取れたものでなければならない。

認識５．(企業ごとの特色)
情報セキュリティ対策は、企業を取り巻く環境や、長年にわたって培われた企業文化と不可分のものであるから、他から移植して済むものではなく、自ら生み出さねばならない（わが国全体としてみれ

ば、「日本的経営の特色」との整合性が必要である)。

4.2 リスクとコンプライアンスの基本認識

以下の知見を得た。

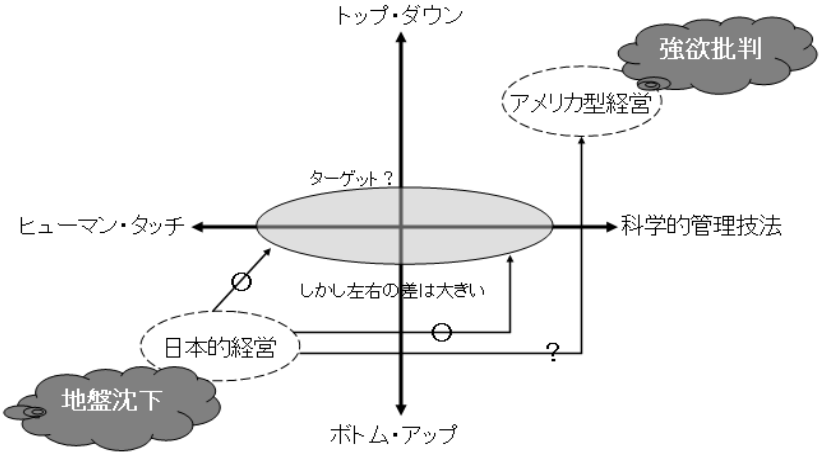
・「リスク」＝経営目標の達成を阻害する恐れのある不確実性を伴う事象およびその要因
・「ビジネス機会」と「リスク」は表裏一体の関係にある。
・リスクを出来る限り合理的に予測、分析、評価して対応を準備することが肝要。
・席上「NHK のプロジェクト X のヒーローは、必ず 1 つや 2 つのコンプライアンス違反を犯している」との発言あり。

出典： 蒲生邦道「内部統制と企業の対応―監査の現場からの問題提起」『2009 年早稲田大学シンポジウム資料』(2009.1.17) を一部修正

この知見は経済産業省の情報セキュリティガバナンスの定義に沿ったリスクとコンプライアンスのあり方と符合しているものと考える。

4.3 情報セキュリティガバナンス手法のベストミックス

認識 5 に関連して、今後の情報セキュリティガバナンス手法のベストミックスを下図の枠組みで検討する必要もあると考える。



4.4 Awareness 提言に基づく Action Plan

4.1 経営者向け

過半を占める事務系出身の経営者に対して、awareness を喚起する運動を 2010 年 2 月から始動した。

4.2 ビジネス・スクール向け

アメリカと同様、ビジネス・スクールのコースの一環として、情報セキュリティを組み込む運動を既に始動した。

5 個別提言

以上のような研究を踏まえて、以下の提言を行った。具体的内容は第 5 編参照。

5.1 情報セキュリティガバナンスのあり方に関する提言

提言 1：外部委託と情報セキュリティ対策
提言 2：アジアへ進出している日系企業の情報セキュリティマネジメント対策
提言 3：情報セキュリティと内部統制規制のあり方

5.2 シグナル情報に関する提言

提言 4：第三者認証制度に求められる 8 原則
提言 5：見えないものの品質保証

提言 6：表示に伴う責任論

5.3 情報と情報セキュリティの一般論に関する提言

提言 7：情報セキュリティ強化に資する法制度
提言 8：情報法の客体としての「情報」の捉え方
提言 9：情報漏えいと個人情報保護

第 2 編　理論研究編

1　情報セキュリティとガバナンス

1.1　情報セキュリティガバナンスとは

ガバナンス（governance）とは、管理、制御、制御方法（システム）、支配、統治（control）のことをいう。統治といえば、統べおさめること、主権者が国土および人民を支配することを意味するように、ガバナンス（governance）も統治もどちらも一般に国家や政府のことをまず念頭に浮かべる言葉、概念である。

情報セキュリティガバナンスも、同様に、まず国や地方自治体などの公的部門の活動を連想するがそれに限るものではない。その担い手（主体）は、企業、団体などの民間部門を含むさまざまな組織に及ぶ。情報セキュリティガバナンスは、今日、あらゆる組織が取り組むべき社会的課題の一つである。

本研究では、情報セキュリティガバナンスを「企業」の活動に限定してとりあげることにした。（以下、特に断りのない限り、情報セキュリティガバナンスとは、企業における取り組みという意味で用いる。）

経済産業省においても同様に企業に限定して用いている。平成 21 年 5 月に『情報セキュリティガバナンス導入ガイダンス（案)』の「情報セキュリティガバナンス」の定義がそれである。少々長いが、引用してみよう。

> 企業の経営陣（代表取締役、取締役、役員等)は、企業価値向上と社会的責任の遂行を目的として、経営や業務の執行に取り組む。その上で、経営陣が適法性・適正性のいずれの観点からも取り組まなければならない活動の一つに、リスク管理がある。経営陣が対峙しなければならないリスクは多様であるが、業種・業態・保有情報等によっては、情報資産に係るリスクが重大なものに位置付けられることがある。
>
> つまり、経営陣においては情報資産に係る機密性、完全性、可用性の観点からのリスク管理を、自らの経営課題の一つとして捉え直すことが重要である。すなわち、様々なリスクのうち、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み（経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組み）を構築・運用すべきである。産業構造審議会情報セキュリティ基本問題委員会では、この取組を「情報セキュリティガバナンス」と定義している。[1]

ここでは「情報セキュリティガバナンス」の考え方を示しているが、その定義において、すでにガバナンスの主体を企業に限定している。本研究における「情報セキュリティガバナンス」の考え方も基本的にここで示されたものと同じである。

1.2　コーポレートガバナンス（企業統治）とマネジメント（管理）

上記の報告書の定義中にも「リスク管理」という言葉が出てくるように、ガバナンス（governance、統治）とマネジメント（management、管理）という概念の用法もまたさまざまである。いかに定義するかという用語法上の問題ともいえるが、研究対象の捉え方や分析のあり方とも関係する重要な概念である。

例えば、組織における意思決定のレベルを、ガバナンス・レベルとマネジメント・レベルに分類した場合、ガバナンス・レベルの意思決定の主体は、組織の実質的所有者、マネジメント・レベルのそれは、ガバナンス・レベルから組織の管理・運営の権限と責任を委ねられた者と捉えることができる。桜内文昭は、前者の例として、株式会社における株主、後者の例としては、株式会社における代表取締役及び取締役会をあげるが[2]、ここでは、経済産業省『情報セキュリティガ

---

[1] 産業構造審議会情報セキュリティ基本問題委員会「中間とりまとめ～企業における戦略的な情報セキュリティガバナンスの確立に向けて～」, 2008/06 http://www.meti.go.jp/press/20080620005/20080620005.html

[2] 桜内文城 著『公会計　国家の意思決定とガバナンス』（ＮＴＴ出版）５頁参照。本項の記述は同書に

バナンス導入ガイダンス（案)』に従い、コーポレートガバナンスとは、「『株主による経営層の統治』と『経営層による企業内統治』の二重の統治構造により成り立つものであって、『株主による経営層の統治』が有効に機能するためには、『経営層による企業内統治』が有効に行われることが前提となる」[3]ものをいう、と捉えることにしたい。

したがって、ガバナンス・レベルの意思決定の主体は、組織の実質的所有者と経営層である。株式会社においては株主と代表取締役・取締役会ということになる。意思決定の対象は、組織の命運に重大な影響を及ぼすような事項、組織の存在意義や使命等長期的な目標の設定（例：定款の目的の設定)，人材や資金等資源の調達・配分（例：合併，営業譲渡，授権資本枠の設定）などがあろう。情報セキュリティガバナンスにおいてもこれと同等のレベルで意思決定を行うことになる。

一方、マネジメント・レベルの意思決定の主体は、ガバナンス・レベルから組織の管理・運営の権限と責任を委ねられた者である。株式会社における執行役以下の管理職がそれである。意思決定及び業務執行の対象は、ガバナンス・レベルによって設定された権限と予算の範囲内で具体的に測定可能な成果の目標を設定し，その目標の達成のため必要な事項について意思決定及び業務執行を行うことである。

ガバナンス・レベルの意思決定がマネジメント・レベルの意思決定を規律付ける関係にある。上述したことを図にまとめると次のとおりとなる。

図　ガバナンス・レベルとマネジメント・レベル[4]

ガバナンス・レベルの意思決定	
意思決定の主体	**組織の実質的所有者（株主）と経営層** **例)**・株主による経営層の統治 ・経営層（**代表取締役及び取締役会**）による企業内統治
意思決定の対象	**組織の命運に重大な影響を及ぼすような事項** **組織の存在意義や使命等長期的な目標の設定（例：定款の目的の設定)，人材や資金等資源の調達・配分（例：合併，営業譲渡，授権資本枠の設定）**

方向付け　**規律付け**

マネジメント・レベルの意思決定	
意思決定の主体	**ガバナンス・レベルから組織の管理・運営の権限と責任を委ねられた者** **例：株式会社における執行役以下の管理職**
意思決定及び業務執行の対象	**ガバナンス・レベルによって設定された権限と予算の範囲内で具体的に測定可能な成果の目標を設定し，その目標の達成のため必要な事項について意思決定及び業務執行を行う。**

ガバナンス・レベルの意思決定がマネジメント･レベルの意思決定を規律付ける関係にある

以上の点を踏まえて、本研究における、情報セキュリティガバナンスについて定義すると次のとおりとなる。

情報セキュリティガバナンスとは、株主（及び株主総会)、経営層（代表取締役・取締役会）が、組織（株式会社）全体の情報セキュリティ(Information Security)が適法かつ適正に維持されるために必要な意思決定を行い、情報の「機密性」(Confidentiality)、「完全性」(Integrity)、「可用性」(Availability)の観点からのリスク・マネジメント（管理）が適法・適正に維持され、か

負うところが大きい。なお，Drucker, P. F.著（田中弥生訳)『非営利組織の成果重視マネジメント：NPO・行政・公益法人のための自己評価手法』（ダイヤモンド社，2000 年）参照。

[3]経済産業省『情報セキュリティガバナンス導入ガイダンス（案)』、2009 年 5 月、間藤大和、平野俊明、中村直人『監査役ハンドブック』、2007 年 10 月参照

[4]　桜内前掲書 5 頁の図表 1 を基に、本稿の採用する定義に従い意思決定の主体の定義と例を書き換えた。

つ業務が円滑に遂行されるための人材の獲得、仕組みづくり（内部組織と権限の付与）、資金等資源の調達とそれを支える要員の意識づくりを行うこと、及びそれに基づき執行役及び管理職が具体的に測定可能な成果の目標を設定し，その目標の達成のため必要な事項について意思決定及び業務執行が行われているかどうかを監督し、これらの結果についての経営責任を負うことをいう。

2　情報セキュリティガバナンスにおける表示と法的責任

2.1　情報セキュリティと法的問題

2.1.1　法的責任の主体・客体

本章では、1 で述べた概念整理に基づき、民事責任、刑事責任、行政法上の責任に関する一般論として、主体、客体、根拠、内容を整理する。

本研究のタイトルは、「企業における情報セキュリティの実効性あるガバナンス制度のあり方」であることから、法的責任の主体は、企業、すなわち法人であり、客体は情報である。ただし、客体たる情報を直接に定義した規定は存在せず、個別の法律の中で、それに関連する定めが置かれている。例えば、個人情報の保護に関する法律 2 条 1 項は「この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう」と定義する。

この点を前提に、法人の法的責任について、民事責任、刑事責任、行政責任に分類すると、次のように整理することができる。

2.1.1.1　民事責任

法人とは、自然人以外で、法律上、権利義務の主体となることを認められたものをいい、法人には権利能力が認められる。

民法 34 条は、「法人は、法令の規定に従い、定款その他の基本約款で定められた目的の範囲内において、権利を有し、義務を負う」と定める。古くは、この「目的の範囲内」の解釈をめぐって議論が存在したが、判例は広く解釈している(八幡製鉄事件最判昭和 27 年 2 月 15 日民集 6 巻 2 号 77 頁)。

また、法人の行為能力の有無は、法人の本質論との関係で、1 つの論点とされてきた。大きく分けると、法人否認説(法人が独自の社会的実体であることを否定する見解)、法人擬制説(自然人意外で権利義務の主体となり得るのは、法律の力によって擬制されたものとする見解)、法人実在説(法人は社会的実体として実在しているとする見解)が存在する。法人否認説、法人擬制説によれば、法人の意思、行為、不法行為能力は否定されるが、現在、この争点はあまり問題とされておらず、法人実在説によって、個人のみならず法人も行為能力を持つことが当然の前提とされている[5]。

2.1.1.2　刑事責任

責任主体は、原則として自然人である。その根拠として、(a)法人には意思に基づく身体の動静がない以上、「行為」は考えられず、(b)主体的・倫理的自己決定もなく、倫理的な責任非難ができない、(c)現行刑法は生命刑・自由刑が中心である以上、法人には適用し得ない、(d)法人には刑罰感受能力が欠けていることが挙げられてきた。判例も、従来から、法人処罰は「他人の行為についての無過失責任」であるという立場を採用してきた(大判昭和 10 年 11 月 25 日大審院刑集第 14 巻 1217 頁)。

しかし、次第に、法人自体の責任を問うべきであるという見解が有力化した。従来の考え方に対しては、(a)´法人に自然人と全く同様の意思に基づく身体の動静はあり得ないが、それでも犯罪の主体とすることは可能である、(b)´刑罰にとって倫理的な非難は本質的問題ではなく、処罰を国民が納得し得ればそれで足りる、(c)´現行刑法典は自然人を念頭に刑罰の種類を設定したため自由刑が多いが、罰金刑も存在し、これは法人にも科し得るといった反論がなされており、現在では、法人の犯罪能力を正面から肯定する立場が有力となっている。その後の判例においても、自然人である事業主の過失を問うもの(最判昭和 32 年 11 月 27 日刑集 11 巻 12 号 3113 頁)、法人

[5] 法人に関する詳しい解説は、内田貴『民法□』(東京大学出版会、第 4 版、2008 年)207 頁以下。なお、法人に関する規定(38～84 条)は、新しい非営利法人制度を定めた「一般社団・財団法人法」、「認定法」、「整備法」の施行に伴い、平成 18 年 6 月 2 日法律第 50 号によって削除された。

自身の過失を問題にするもの(最判昭和 40 年 3 月 26 日刑集 19 巻 2 号 83 頁)が登場した。とりわけ後者について、最高裁判所は、「事業主が人である場合の両罰規定については、その代理人、使用人その他の従業者の違反行為に対し、事業主に右行為者らの選任、監督その他違反行為を防止するために必要な注意を尽さなかつた過失の存在を推定したものであって、事業主において右に関する注意を尽したことの証明がなされない限り、事業主もまた刑責を免れ得ないとする法意と解するを相当とすることは、すでに当裁判所屡次の判例…の説示するところであり、右法意は、本件のように事業主が法人(株式会社)で、行為者が、その代表者でない、従業者である場合にも、当然推及されるべきである」と判示した。

刑法典には法人処罰に関する特別の規定は存在しないものの、行政刑法には法人を処罰するものが多い(所得税法 244 条、外国為替及び外国貿易法 72 条、人の健康に係る公害犯罪の処罰に関する法律 4 条等)。もっとも、現在認められている法人処罰は、あくまで、個人を処罰した場合にあわせて法人を処罰するという両罰規定であることに注意しなければならない。法人は、従業員が業務に関し犯罪を犯した場合にのみ罰金を科されるに過ぎない。その意味で、「個人責任なくば企業責任なし」の原則が妥当している[6]。

現行法では、法人には罰金刑しか科し得ないが、法人自身に対する刑事責任は、立法論を示唆する課題といえる。

2.1.1.3　行政責任

法人は、民事上、刑事上の責任主体になるとともに、行政法上の責任主体でもある。

行政法とは、文字どおり「行政」に関する法である。その名称に「行政」の 2 文字を含む法律は 120 を超えるが、民法典や刑法典のように、「行政法」という通則的法典は存在しない。他方、現行の約 1800 の法律の大半は行政法に関連するといわれる。したがって、法人が行政法上の責任を負うケースは多く、その責任内容については、個別具体的な法律を対象に考える必要がある。

また、行政法は、その性質から、行政組織法、行政作用法、行政救済法に分類して説明される。このうち、行政作用法は、「行政主体(国、地方公共団体等)が、行政機関を通じて私人に対して行う行政活動をめぐって生ずる権利義務関係を起立する法」をいう。「私人」には法人も含まれる。例えば、個人情報の保護に関する法律、特定電子メールの送信の適正化等に関する法律、特定商取引法、電気通信事業法や有線電気通信法等の通信関連法は、行政作用法に属する。

なお、法律の定めによって、日本国の法人のみに権利能力が認められる場合もある。鉱業法 17 条「日本国民又は日本国法人でなければ、鉱業権者となることができない。但し、条約に別段の定があるときは、この限りでない」と規定している。

2.1.2　法的責任の根拠

2.1.2.1　民事責任

民法上の責任は、不法行為及び債務不履行責任である。

債務不履行の根拠規定は、民法 415 条であり、契約に違反した法人は、この定めにより責任を問われる。

例えば、レンタルサーバ消失事件(東京地判平成 13 年 9 月 28 日別冊 NBL79 号 16 頁)では、被告プロバイダが自己のサーバに保管していた原告のホームページのファイルを消滅させた事案であり、被告に対し、レンタルサーバのサービス契約にかかる債務不履行に基づく損害賠償の支払いが命じられた(バックアップコピー等を取っていなかったことにより 5 割の過失相殺)。

開発したソフトウェアプログラムの瑕疵・完成の遅滞が発生した場合も、債務不履行責任が問題となる。これは、ユーザ企業から開発を委託されて、システムベンダが作成したソフトウェアプログラム又はそれを含めて構築したシステムに、重大な瑕疵(不具合・欠陥・バグ)が存在し、その結果、瑕疵のために使用に耐えず、又は完成期限を徒過して稼働に至らないという紛争である。開発委託契約は、民法の典型契約には含まれないが、裁判例の趨勢は、請負契約として分類している。したがって、ベンダは、通常の債務不履行責任以外に、瑕疵担保責任を問われる場合がある[7]。

不法行為責任については、法人自身が当事者となり直接に責任を負う場合、及び、被用者が第

---

[6] 以上、前田雅英『刑法総論講義』(東京大学出版会、第 4 版、2006 年)98～100 頁。その他、企業組織体責任論という考え方も存在する。これは、企業組織体の活動を、個人の行為とは独立に全体的に捉えて行動基準違反の有無を論じた後に、各個人の立場に応じて責任を割り付けていくという考え方であり、過失論に限定して論じられている。しかし、立法論としてはともかく、解釈論としては採用しがたいとの批判されている。

[7] 岡村久道『情報セキュリティの法律』(商事法務、2007 年) 234 頁～242 頁。

三者に加えた損害について、監督責任を負う場合に分けられる。前者は民法 709 条の一般の不法行為責任、後者は 715 条の使用者責任である。

不法行為責任は、故意又は過失に基づく人の行為によって生じるものであり(過失責任の原則)、その結果発生する責任は、行為者本人が負う(自己責任の原則)のが原則である。しかし、社会の発展に伴い、これらの原則を貫徹すると不都合・不公正が生じるため、特に法人の活動等についてはある程度の無過失責任を認めるべきであるとの考え、すなわち、報償責任主義や危険責任主義のもと、民法 714 条以下には特殊的不法行為の規定が置かれている。使用者責任は、報償責任主義に基づくといわれている。

また、企業の日常的な活動から生じる損害の場合、現代の大企業の複雑な人的組織・意思決定機構を考えると、使用者責任ではなく、企業を全体の加害者と捉えて、企業自身の 709 条に基づく不法行為責任を問題とする考え方が存在し、これを企業責任と呼んでいる。この考え方は、公害、製造物責任の分野では古くから採用されており、報道機関等による名誉毀損に対しても、会社自体の 709 条責任が問われるケースが多い。企業責任は、個々の被用者の過失を問題にすることに意味がない類型の不法行為に対して、企業自身の不法行為責任を認めようとするものである。

例えば、機密性侵害によって、民法 709 条の責任が問われたケースとして、Yahoo!BB 個人情報漏えい事件(大阪地判平成 18 年 5 月 19 日判時 1948 号 122 頁、大阪高判平成 19 年 6 月 21 日公刊物未登載)がある。この事件では、BB テクノロジーの業務委託先の元従業員及びその知人において、共有アカウントを用いて外部から不正にアクセスし、Yahoo!BB の会員情報を取得したことが問題となったが、被告 BB テクノロジー株式会社及び同ヤフー株式会社に対し、共同不法行為に基づく損害賠償の支払いが認められている。

一方、TBC 個人情報漏えい事件(東京地判平成 19 年 2 月 8 日判時 1964 号 113 頁、東京高判平成 19 年 8 月 28 日判タ 1264 号 299 頁)では、TBC が委託先を通じて開設していたウェブサイトにおいて実施されたアンケート等の回答結果が、インターネット上に流出し、被害者から損害賠償を求められた。この事件では、民法 709 条及び 715 条 1 項が選択的に請求され、東京地方裁判所は、使用者責任を認めて TBC に損害賠償の支払いを命じた。

なお、715 条 1 項の定める「被用者」は、個人に限るものではない。東京地裁は、原告の主張を認め、委託先企業を「被用者」と評価し、その不法行為責任を認め、TBC には選任監督上の過失があったと認定している。本件では、委託先企業は被告とはならなかったが、共同不法行為責任(719 条)を問われることも十分あり得た事案である。

したがって、企業としては、自らが委託元となる場合はもちろん、委託先となる場合にも、実体法上は不法行為責任を負うこととなる。

さらに、法人の行為が他者の名誉やプライバシーなどの人格権を侵害する場合がある。

人格権とは、法的保護の対象となる人格的利益の総称をいう。人格権は、排他性を有する絶対権的性質を持つと理解されていることから、その侵害に対しては差止命令が認められる(『北方ジャーナル』事件最判昭和 61 年 6 月 11 日民集 40 巻 4 号 872 頁)。差止命令に行為者の故意・過失は必要とされない。

以上のように、民事責任は、加害者に故意がある場合に限らず、過失が存在していれば損害賠償責任が認められ、さらには、人格権侵害の場合は過失も要件とされない。したがって、故意責任の原則を採用する刑法(38 条 1 項)と比較すれば、その責任範囲は広い。

2.1.2.2 刑事責任

刑事責任の根拠は、刑事処罰を定める各法律の規定であり、1 つ 1 つの犯罪行為につき、構成要件、違法性、有責性を満たすことが必要である。しかし、我が国の刑法典、ことに財産犯に関する規定は、有体物を中心に構成されている。したがって、電子データの入った物理媒体や紙の占有を侵奪した場合は窃盗罪が成立し(235 条)、信頼関係に違背して領得した場合は業務上横領罪(253 条)等が成立する。

しかし、物理媒体や紙ではなく、データそのものを盗んだ場合、伝統的な刑法の規定では救済を図ることはできない。裁判例上も、あくまで他人の媒体に保存されたデータを不正に得た場合に、その媒体に対する財産犯が成立するという構成を取っている(新潟鉄工事件東京高判昭和 60 年 12 月 4 日刑月 17 巻 12 号 1171 頁、京王百貨店事件東京地判昭和 62 年 9 月 30 日判時 1250 号 144 頁、城南信金不正告発事件東京地判平成 9 年 12 月 5 日判時 1634 号 155 頁等)。したがって、自分が管理する勤務先の顧客データを無断で電子メールの添付ファイルとして送信した場合には、「物」を領得したことにはならず、同様に、自分が持ってきた媒体にデータを保存して持ち出し

た場合にも、「他人の」物の領得にはならないため、財産犯は成立しない。

また、強盗罪、詐欺罪、恐喝罪には、2 項が存在しており、有体物ではなく「財産上不法の利益」を得た場合にも成立する。しかし、学説上は、強盗罪、詐欺罪、恐喝罪は移転罪であって、情報が不正に取得されたとしても、その情報を保有していた者も、引き続き同じ情報を持つことができることから、移転したとはいえないとして、否定的に解釈する説が有力である。

一方、刑法は、コンピュータ処理による不正行為に対処するため、1987 年に改正され、電磁的記録(7 条の 2)関連の犯罪類型を、偽変造罪(157 条以下)、業務妨害罪(234 条の 2)、詐欺罪(246 条の 2)、毀棄罪(258 条、259 条)の中に盛り込んだ。これは、実質的な意味で、情報セキュリティに関連した日本初の法整備といわれている。2001 年には、支払用カード電磁的記録に関する罪が成立した(163 条の 2)。その後、2004 年にサイバー犯罪条約を国内法化するための刑法改正法案として、犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案が提出されたものの、現在に至るも継続審議中である。この法案は不正指令電磁的記録作成等の罪を定めており、ウイルス作成、提供、取得、保管等を犯罪の対象にしている。

また、刑法典には、情報の機密性を侵害する行為を本来の処罰対象とする規定として、秘密漏示罪(134 条)、信書開封罪(133 条)等が存在するが、これらは数少ない例外にとどまる[8]。

不正アクセス禁止法は、ネットワーク上の不正行為に対処すべく、1999 年に制定された。同法は、アクセス制御機能を持つ電子計算機にアクセスし、他人の ID や PW を入力するなどして、その制限されている特定利用をし得る状態にさせる行為を処罰対象とする。

2.1.2.3 行政責任

行政法上の責任の根拠は、各法律の定めによる。例えば、個人情報保護法は、個人情報取扱事業者に対し、利用目的の特定(15 条)、利用目的による制限(16 条)、利用目的の通知等(18 条)、安全管理措置(20 条～22 条)、第三者提供の制限(23 条)、開示、訂正等、利用停止等(25 条以下)の義務などを課しており、違反をすれば、主務大臣から報告を求められ、助言、勧告、命令を受けることがある(32 条以下)。特定電子メール法は、特定電子メールの送信について、事前に要請又は同意をした者に対してのみ送信を行うことを原則とし(3 条)、また、電子メール上に所定事項を表示すること(4 条)等を定めている。違反した送信者は、総務大臣から措置命令を受けることがある(7 条)。

行政法が何であるかについては、必ずしも統一的な見解が存在するわけではない。しかし、行政法の存在意義・役割は、主に、次のように説明されている。

行政法という 1 つの法分野を他の分野から区別する以上、そこでは、他の分野では通常正面から取り上げられることのない法現象・法関係が取り扱われることになる。例えば、税金の賦課徴収や土地の公用収用などの場合には、行政主体の側には、相手方当事者である納税者や土地所有者の同意がなくとも、最終的には一方的に税金の納付の義務を課し、あるいは土地の所有権を変動せしめる権限が、法律上与えられており、また、相手方がそれに従わない場合には自ら強制力をもってそれを実現する権能が与えられている。行政活動に際し、とりわけ行政行為を中心的手段として公権力の行使が行われる場合については、行政主体と私人との間には、通常の私人間相互の法関係とはその内容を異にする法関係が存在する。このような、私人間相互には通常見られない法関係を規律する法は、「行政に特殊固有の法」、「行政に関する公法」などと呼ばれてきた。

また、公法・私法二元論との関係でいえば、行政活動は基本的には「公法」によって規律されている。しかし、国や地方公共団体が土木建設会社に工事を発注する場合のように、行政をめぐる法関係が全て「公法」によって規律されているとはいえない。行政に関する諸々の法規範の中に、行政法という特別の法分野を形成する法規範と、民法、商法、刑法等の分野に既に吸収される法規範の別が存在する[9]。

その他、行政法は、民事、刑事による処理だけでは足りない部分を補うところに意味を持つという見解も存在する。そこでは、民事賠償だけでは、後始末的解決にならざるを得ず、刑事法的手法では、刑罰で取り締まるか放置するかの「白か黒」になるので、融通が利かない。そこで、行政法は、先手を打って規制を行うことを通じて、問題の発生自体を極力減少させ、うまく社会を管理することを 1 つの役割とする[10]と説明されている。

---

[8] 以上、岡村・前掲『情報セキュリティの法律』78 頁以下参照。

[9] 藤田宙靖『行政法 I』(青林書院、第 4 版、2003 年)25 頁以下。

[10] 以上、稲葉馨ほか『行政法』(有斐閣、2007 年) 2～3 頁。

例えば、個人情報保護法は、個人情報の不正な取扱いを未然に防止し、特定電子メール法は、一時に多数の者に対してされる迷惑メールを規制することにより、インターネット社会を良好な環境に保つことを趣旨とする。

2.1.2.4　その他

その他、著作権法や不正競争防止法等、個別の法律によって、民事責任ないしは刑事責任が認められる。

ただし、民事、刑事、行政の 3 つの法分野は、孤立して存在しているわけではなく、むしろ、様々な場面で交錯している。刑事法と行政法の関係を見ると、主務大臣の命令や総務大臣の措置命令に違反すれば刑事罰が科せられるように、行政法上の義務は刑事罰によって担保されている。民事法との関係では、法の一般原則が表明されているような民事法の規定(信義誠実の原則、権利濫用の禁止等)は、行政法上の法律関係にも適用される[11]。

また、例えば、電気通信事業法 9 条、有線電気通信法 4 条、電波法 59 条は、通信の秘密を侵してはならない旨を規定する。通信関係法は行政法に位置づけられるが、通信の秘密は私人間にも適用される。また、通信の秘密を侵害する行為には罰則(電気通信事業法 179 条、有線電気通信法 14 条、電波法 109 条)が設けられており、刑事法に分類される。

2.1.3　法的責任の内容

2.1.3.1　民事責任

債務不履行の場合は、損害賠償及び契約解除である(415 条、541 条)。

一方、前述した請負契約の担保責任については、明文上、瑕疵修補請求権(民法 634 条 1 項)、損害賠償請求権(同条 2 項)、契約解除権(635 条)が適用される。損害賠償請求権については、瑕疵の修補に代えて、又は、瑕疵の修補とともに請求することが認められる。契約解除は、契約目的が達成不能の重大な瑕疵がある場合に限られるが、催告は要件とされていない。以上の規定は、瑕疵の原因が注文者にある場合は、原則として適用されない(民法 636 条)

不法行為の場合は、損害賠償が原則であるが、民法 723 条において、名誉を回復するのに適当な処分が認められている。

また、名誉、プライバシー等の人格権を侵害した行為に対しては、差止請求が認められる。

2.1.3.2　刑事責任

刑法 9 条は、「死刑、懲役、禁錮、罰金、拘留及び科料を主刑とし、没収を付加刑とする」と定める。このうち、法人に科しうるのは罰金のみである。

2.1.3.3　行政責任

行政法上の義務履行手段は、代執行、執行罰、直接強制、強制徴収など様々用意されているが、情報セキュリティ関連法の中では、報告聴取、助言、勧告、命令といった手段が用いられている。

報告徴収及び命令は、行政不服審査法上の「処分」に該当することから、同法に基づく不服申立て(行政不服審査法 2 条 1 項、3 条以下)、又は、行政事件訴訟法に基づく処分の取り消しを求めることが可能である(行政事件訴訟法 8 条以下)。処分に該当する場合は、行政手続法は適用除外となる(行政手続法 3 条 1 項一四号)。

助言及び勧告は、行政手続法上の行政指導に該当する(行政手続法 2 条六号)。行政指導に携わる者は、趣旨、内容、責任者を明確にすることや、書面の交付が義務づけられる(35 条 1 項 2 項)。

2.1.3.4　その他

著作権法及び不正競争防止法は、差止請求権を明文で認めるとともに、擬制侵害、損害額の推定等を定める。これらの法律は、代表者又は従業者の違反行為に対し、法人に 3 億円以下の罰金刑に処する両罰規定を置いている。

以上、法人の責任をめぐる一般論を述べてきた。法人責任をめぐる論点はいまだ突き詰めて検討されておらず、従来は、個人に責任を負わせる場合に法人にも責任を及ぼすべきか否かという視点から議論されてきた。しかし、今後は、逆の発想に立脚し、①そもそも法人に責任を負わせるべきか否か、②法人に責任を負わせるべき場合に、個人に責任を割り付けるべきか否かという観点での検討も必要と考えられる。

2.2　表示と法的責任をめぐる論点整理

2.2.1　コミットメント責任と表示責任―検討のねらい

コミットメント責任とは、一般的な用語ではなく、本研究会において議論の土台とするために

[11] 以上、稲葉ほか・前掲『行政法』3～7 頁。

採用した用語である。ここでは、事業者が事業活動をするにあたって、特定の内容を消費者や取引先などに対して表示し、または不特定多数に宣言したことによって生じる法的及び社会的な責任一般をいう、と定義した。

法的責任を検討する上では、むしろ表示責任といった方がわかりやすい。既存の議論の下で、誰の、誰に対する、どのような責任かを踏まえて検討することが可能だからである。本稿でも、法的責任論においては主に表示責任を用いる。

しかし、すでに一定程度の法的救済の対象となっている問題よりも、むしろ事業者が一方的、自発的に、何らかの約束的なことを社会的に表明したとしても法的な責任が曖昧なまま放置されているところにも光を当てる必要がある。そこでは、社会的責任に拡大して検討が必要であることから、あえてコミットメント責任を用いることがある。

具体的には、情報セキュリティ関連の分野においては、プライバシーマークや ISMS などの認証マークを対外的に示して取引した場合の法的、社会的責任を検討の題材としてとりあげることとした。

消費者や取引先はそれを法的にどのように評価すべきなのか、事業者がその信頼を裏切った場合（例えば情報漏えいをしたような場合）に、認証の取得を事実上信頼したことはどのように法的に評価されるのか、契約内容に関係すれば契約違反を問い、不法行為があればその責任を問い得るというのは当然として、そこに認証取得の事実を告げたことがどのような影響を与えるのか、それとも与えないのか、さらには、認証を信頼しそれによって損害を被った消費者や事業者に対して、認証した機関は、その制度上免責を宣言していれば常に免責されるのであろうか、そこには法的な責任がないのかどうか、あるとしたらどのようなかたちで問われるべきか、といったことが論点となる。

以上の論点は現行法の解釈の中で解決可能か、それとも新たな立法的解決を図る必要があるのか、その場合、どのような背景的な法理論が求められるべきかを検討していかなければならない。事業者が安易に約束的な表明をすることによって多少なりとも信頼という果実を手にいれながら、そこで得た社会的な信頼を無にしたとしても一切の責任が問われないというのもおかしな話だからである。また、そのような認証制度を普及させる政策の是非も検討が必要であろう。

今後の社会は、ソフトローの果たす可能性や NGO の活躍に期待するところが非常に大きくなっていくことが予想されるだけに、こうしたコミットメント責任が問われるべき意義があるように思われる。まさに民間認証制度や格付機関は花盛りであり、いつの間にか社会的な権威性をまとうこともあるが、民間認証はあまりに野放図なままである。目的に公益を掲げ、公的な色彩をまといながら、また行政庁との関係を背景にした信用を得ながら、責任論においては、民民の関係という形式が強調され、民事的解決に委ねるべきものとして放置されている。行政行為であれば、法律による行政の原理の下、常に根拠法が求められ、情報公開法と行政手続法によって規律され、事後は行政救済法によって国民の救済の道が開かれている。

認証制度は多様であり、その実態はブラックボックスのままである。ブラックボックスのまま誰の検証もないまま社会的な信頼の連鎖の下に社会的権威性が保たれているようでもある。民間認証制度や格付機能などの検証をすることなく、単に認証マークの表示の法的、社会的責任を抽象的に論じることはできない。マークの社会的認知度、信頼性は制度ごとにばらばらだからである。

そこで、まず「第三者評価認証制度」とは何かを検討し、さらには、既に１万社近い事業者が認証を取得しているプライバシーマーク制度をとりあげ、詳細にその制度設計、運用実態を調査し、その課題が何かを捉えることとした。また、外部委託における ISMS 認証の活用についても調査検討した。これらは 3 から 5 で述べられている。

したがって、認証マーク等の表示の法的責任、社会的責任についての研究は、今回の研究成果を下に今後とも継続することとして、以下では法的検討を行う上での用語の定義と論点整理を行った。

2.2.2　表示と法的責任

2.2.2.1　「表示」の意義

表示とは、広辞苑によると「外部にあらわし示すこと」であるが、契約責任における表示は、「契約締結の際またはそれ以前に、交渉相手方に対して行う明示または黙示の表明で、交渉相手方に契約に関するさまざまな期待を生じさせるものである。具体的には、商品表示、セールスマ

ンや勧誘員の説明として現れるだけでなく、広告の中にも含まれることがある。」[12]

ここでは事業者の活動として行われる明示的な表明で、その表示を見た者（消費者、取引先等事業者）に対して当該事業者または他人の商品、サービス、その他事業活動一般に関するさまざまな期待を生じさせるものと定義する（黙示的な表明は含まない）。具体的には、個人情報保護方針（プライバシーポリシー）の表示、認証マークの表示、その他事業者の商品、サービス、その他事業活動一般に関するステートメント等の文章の表示などがある。

また、表示の根拠に着目するなら、①法律に基づく表示（義務）がある。②表示自体は義務付けられていないが、表示することによって行政の規制対象となるものもある。それから、③政府の基本方針、ガイドライン、規格等告示に基づく任意的な表示がある。個人情報保護方針（プライバシーポリシー）などがそれである。④事業者の意思に基づく自主的、自発的な表示がある。また、事業者の意思に基づくということにもなるが⑤契約に基づく表示がある。認証制度の中には JIS Q 15001 など告示を審査基準にして契約によってプライバシーマーク等認証マークの表示について義務づけるものがある。

2.2.2.2　表示と契約責任

契約責任で問題とする表示は、「多くの場合、相手方を契約締結に誘因するだけの事実上の表示であるが、売主のなす価格表示が契約申込みの内容となるように、意思表示の内容をなす場合もある」[13]。

表示は、「申込の誘因」と評価される場合と「申込」と評価される場合があり得る。後者の場合は、意思表示における表示行為と「表示」が一致することがある。こうした表示は契約成立により契約合意の内容となり、もしくは、契約の付随義務の内容となる。

その他の表示は単なる「事実行為」として、契約（法律行為）には何ら影響を与えないと評価されることになる。認証マークの表示やプライバシーポリシーの多くは、ここに分類されるものと思われるが、契約的な構成の存在を見出し得るかどうかは、認証制度のあり方やプライバシーポリシーの記述内容など個々のケースによって異なる。

このことが民間認証制度の規律のあり方（完全に民間団体の自由に委ねていいのかどうかという問題）とプライバシーポリシーのあり方としていいのかという政策論上の問題がある。

2.2.2.3　表示と不法行為責任

芸能人が広告に出演する場合、その広告内容を調査する義務があるとし、不法行為責任を認めた判例として高田浩吉事件(大阪地方裁判所昭和 62 年 3 月 30 日判決判タ 638 号 85 頁)がある[14]。いわゆる原野商法に関する事件であるが、芸能人が推薦文の制作に関与したという点に着目するならば、表示と不法行為の問題として捉えることができる。他人の商品、サービスの品質等に対して一定の信用を付与するような表明を行うと、それが事実と著しく異なるものであった場合は、不法行為責任を問われることがあるという意味では、事業者は無論のこと第三者評価認証制度における民間認証機関の法的責任を考える場合においても参考となる判例である。

2.2.3　法律に基づく表示義務と法的責任

法律によって事業者が一定の表示を義務づけられる場合がある。一般に表示の懈怠は義務違反となり行政処分や罰則を科されることになる。例えば「個人情報の保護に関する法律」（以下「個人情報保護法」という。）では、個人情報取扱事業者に対して、本人から直接書面に記載された当該本人の個人情報を取得する場合に利用目的を「明示」（表示）するよう義務付けている（18 条 2 項）。この義務に違反し利用目的の明示をしなかった場合は、主務大臣の報告の徴収、助言、勧告、命令の対象となり(32 条～34 条)、命令に反した場合は、6 月以下の懲役又は 30 万円以下の罰金に処することとなっている(56 条)。

「表示」を義務づける規制が民事責任にどのような影響をもたらすのか。例えば、ここでの明示が「申込の誘因」と評価され、または意思表示における表示行為と「明示」が一致することで「申込」評価されることもあるだろうが、一般的には、こうした取締規定としての表示義務は、契約(法律行為)には直接影響しないと解されるのであろう。

また、ここでは利用目的として明示された内容と、同時に契約約款として示した約定に示された利用目的条項との内容的な齟齬をどう処理するか、利用目的の明示に錯誤、強迫などがあった

---

[12] 藤田寿夫『表示責任と契約法理』（日本評論社、1994）3 頁。本書はここでの検討に際して大変参考になり、多くの示唆を得た。

[13] 藤田前掲書 3 頁。

[14] 判例タイムズ 638 号 85 頁、判例時報 1240 号 45 頁、判例タイムズ 696 号 41 頁

場合の処理に民法の意思表示の規定を準用し得るのか、利用目的の変更(15 条 2 項)及び目的外利用の規制(16 条 1 項)との解釈との関係が問われることにもなる。

その他、情報セキュリティとの関係においては、特定電子メール法、特定商取引法上の表示義務などにも表示の問題をみることができる。

2.2.4 政府の基本方針、ガイドライン、規格等（告示）に基づく任意的な表示と法的責任

内閣府は個人情報保護法に基づき、「個人情報保護に関する基本方針」を告示しているが、そこでは、(1) 個人情報取扱事業者に関する事項 ①事業者が行う措置の対外的明確化として「事業者が個人情報保護を推進する上での考え方や方針(いわゆる、プライバシーポリシー、プライバシーステートメント等)を策定・公表することにより、個人情報を目的外に利用しないことや苦情処理に適切に取り組むこと等を宣言するとともに、事業者が関係法令等を遵守し、利用目的の通知・公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要である」としているほか、主務大臣もそれを受けて個人情報保護ガイドラインにその旨を踏まえた条項を用意し、事業者に「個人情報保護方針」の公表(表示)を求めている。さらには、経済産業大臣は、工業標準化法に基づき「JIS Q 15001 個人情報保護マネジメントシステムー要求事項」を策定し、その要求事項 3.2 個人情報保護方針において「事業者の代表者は、個人情報保護の理念を明確にした上で、次の事項を含む個人情報保護方針を定めるとともに、これを実行し、かつ、維持しなければならない」とし、6 項目の表示事項を例示列挙している。JIS Q 15001 は後述するようにプライバシーマーク制度の審査基準として、同マークの取得を必要とする事業者においては、個人情報保護方針の策定と公表(表示)は必須事項となっている (4 参照)。

個人情報保護方針(プライバシーポリシー)の公表(表示)は「申込の誘因」または「申込」と評価され契約責任として捉えることができるのかどうかは、その記述内容におうところが大きく、一般的抽象的に論じることはできない。しかし、契約責任を問い得ない場合でも、こうした背景をもって事業者が社会に宣言する内容が単なる一文書にすぎないというのも、消費者保護の実質があまりに乏しく制度のあり方として問題があるように思われる。

例えば、米国の連邦取引委員会法(FTC 法)第５条(a)は、いくつかの法改正により、不公正な競争方法(unfair methods of competition)のほか、不公正・欺瞞的な行為又は慣行(unfair or deceptive acts or practices)を禁止しており、後者により FTC はいわゆる消費者保護行政も所管している。この点、事業者がプライバシーポリシーやステートメントを表示することで、消費者の信頼を得ていたにも関わらず、その内容に反する行為を行うなど、消費者に対する欺瞞的行為を行った場合に、連邦取引委員会(FTC)が当該事業者に調査を行うことができる。事業者の側は、漫然とプライバシーポリシーを策定し公表（表示）することはできない。そこには行政の介入を招く法的リスクがあるからである。

さて、日本においては、いわゆる個人情報保護方針(プライバシーポリシー)にきれいごとを書き並べ、消費者を信頼させた上で、それに反するビジネスをしている事業者に対して、行政はどのような関与が可能なのであろうか。プライバシーマークと個人情報保護方針(プライバシーポリシー)を表示して、それに反する活動をしている事業者に対してはどうであろうか。日本の公正取引委員会は、現行景品表示法によって介入することは可能なのか。個人情報保護法における主務大臣の関与のあり方は十分なのかが問われなければならない。

このあたりが不明確であるとしたら、個人情報保護方針(プライバシーポリシー)を表示することを推奨する現在の個人情報保護法制は、いったい何をどこまで実現することをねらいとしているのかはなはだ疑問となってくるのである。同種の表示は、そのほかにもいろいろあり得るところであり、法的責任から離れた紙切れがいくら表示されてもその実益はあまりに乏しいというほかなく、その政策や認証制度はあまりにも虚しいものであろう。企業の情報ガバナンスに資するところもわずかである。

2.2.5 表示と第三者評価認証制度(民間認証制度)

2.2.5.1 認証マークを表示した事業者の法的責任

すでに述べたところであるが、例えば、プライバシーマーク制度、ISMS 制度など第三者評価認証制度における認証を取得した事業者が認証マークを「表示」して業務を行っていた場合、その認証を信頼し取引に応じた消費者や取引先に対する法的責任の有無が問題となる。

プライバシーマークを表示して、JIS Q 15001 に準拠した運用をすることを社会に宣言していた(もしくは、顧客に表示していた)事業者が、顧客の個人情報を取得した後、JIS Q 15001 に反

する運営をしたことが原因で当該個人情報を流出した場合、それを信頼して個人情報を提供した本人は、当該事業者に対してどのような法的責任を負うのかということである。あくまでも事実上の判断材料にすぎないということで許されるのかどうかという問題でもある。

2.2.5.2 第三者評価認証制度(プライバシーマーク制度、ISMS 制度など)における第三者評価機関の認証責任

例えば、プライバシーマーク制度を主宰する(財)日本情報処理開発協会(JIPDEC)が認証を与えたことの法的責任をどのように評価するかといった問題である。認証制度が社会に広く認知され、事実上取引の条件として機能してきた場合は特にこの点が問題になってくる。個人情報を流出したプライバシーマーク取得事業者に充分な資力がないような場合は、 JIPDEC が認証を与えたことの法的責任をあわせて問われるということもあるだろう。

JIPDEC は、何を認証しているのか。JIPDEC は、どこまでの範囲で法的責任を負うのか。上述の点が不明確でも、それは第三者評価認証制度といえるのか。民間認証制度は、自ら認証制度だと名乗りを上げれば、誰でも認証業務を行えるのか。一切の法的責任を負わない形で制度設計することも可能であろうが、それはそれを見抜かずに安易に取得した事業者やそれを調査しない消費者、取引先の問題でしかないのだろうか。認証マークの表示の法的責任を論じる前に、認証機関の責任、民間の第三者評価制度の意義とあり方、要件の問題、認証機関の監督のあり方の問題が大きく横たわっている。

本問題は、3 以下で述べる第三者評価認証制度の研究の成果を踏まえて、さらに継続して取り組む必要がある。

3　第三者評価認証制度

3.1　第三者評価認証制度とは何か

3.1.1　第三者評価認証制度とは

「第三者評価・認証制度」とは、一般的に、製品若しくはサービス、又は、組織としての方針や目的を達成するための仕組みを適切に運用するためのマネジメントシステム等に関し、一定の手続きによって定められた規格・基準に適合しているかどうかを評価する制度をいう。「認証」（Certification）とは、製品、プロセス、サービスが特定の要求事項に適合していることを第三者が文書で保証する手続をいう場合が多い（電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）（以下「電子署名法」という。）における「認証」業務は、たとえば、公開鍵暗号方式を用いた電子署名の場合については、電子署名に用いられる署名(秘密)鍵に対応する検証（公開）鍵が特定の者に関係づけられることを証明する業務を言うものと定義づけられており（同法第２条第２項)、規格・基準への適合性ではなく、電子署名の作成者の確認のために用いられる公開鍵とその公開鍵で検証される秘密鍵が帰属する個人との結びつきの確からしさを証明するものであり、その認証書が電子的な署名検証を可能にする技術様式による電子データとして一定の基準に従った方式で発行されなければならないものであることから、「電子認証」とも呼称され、いわゆる適合性評価制度における認証とは意味を異にする。)。

なお、類似の用語として、「認定」(Accreditation）が用いられることがあるが、「認定」は、第三者機関として認証を行う機関に関し、その機関が適合性評価業務を行うために必要となる品質マネジメント、業務の実施方法、要員など規格・基準を満たしていることを証明することをいう。適合性評価のための試験や認証等を行う認証（試験）機関の適合性を証明する組織が認定機関と呼ばれる（なお、ここにおいても、電子署名法による特定認証業務の「認定」は、認証「機関」の適合性の認定ではなく、「認証業務」自体が同法の施行規則等に定められる基準を満たすものであることを証明する行為をいい、いわゆる適合性評価制度における認定とは意味を異にする。)。

第三者による評価・認証が必要とされる場合とは、たとえば、製品の安全性や一定のリスクに対する組織の対策状況等、外観上そのレベルが必ずしも明らかにならないものについて、製品やサービスを提供する者が、自らの提供する製品やサービスが一定の規格や基準を満たしているものであることを示す必要がある、または示すことにメリットがある場合であるといえ、評価・認証に要するコストは、製品やサービスを提供する事業者において負担されるのが通常である。製品やサービスを購入、利用しようとする者が、その製品やサービス、プロセス等の品質、安全性等を、独自に調査、検討、評価することは、評価に必要となる専門知識や環境を備えるコストの負担を多数が重複して行うことにつながり、特に汎用的な消費財について消費者側にそのような負担を強いることは、合理的でない。また、そのような負担は、利用者側が新たな製品、サービスの利用に躊躇する原因となり得、市場による合理的な競争を妨げる要因ともなり得る。さらには、国境を越える取引においては、国際標準への適合性に関し、国際標準に則った方式・手続きによる適合性評価・認証を受けることが競争力の観点から重要になる場合があり得る。

このような観点から、①法律によって、利用に当って人の生命や身体の安全に対するリスクを伴うような製品等について、一定の基準に適合することが確認（認証）されなければ製造、販売を禁止する制度が設けられたり、②製品等の品質の改善、生産能率の増進、生産の合理化、取引の単純公正化、使用・消費の合理化のために、法律によって規格・基準の定め方や、その規格・基準への適合性の認証の方法が規律されたり、③法律の規定による根拠を伴わないが、安全性の高い製品･サービスの流通や､利用者の選択の合理化のための民間による適合性評価制度が構築、運用されたりする等、様々な適合性評価・認証制度が運用されている。

情報セキュリティに関する第三者評価・認証制度としては、情報セキュリティマネジメントシステムに関する適合性評価制度（ISMS 適合性評価制度)、プライバシーマーク制度、IT セキュリティ評価及び認証制度（ISO/IEC15408)、及び、暗号モジュール試験及び認証制度（JCMVP)、ならびに、適合性評価制度とは趣を異にするものではあるが、「電子署名及び認証業務に関する法律」による認証業務及び特定認証業務の特定認証業務等がある。

3.1.2　参考となり得る情報セキュリティ以外に関する第三者評価・認証、表示制度

3.1.2.1 工業標準化法に基づく JIS マーク表示制度

第三者による評価認証制度として認知度が高いものとしては、工業標準化法（昭和 24 年法律第 185 号）に基づく手続によって制定される「JIS マーク表示制度」の制度がある。

「JIS マーク表示制度」は、「鉱工業品の品質の改善、生産能率の増進、生産の合理化、取引の単純公正化及び使用又は消費の合理化を図ること」等を目的として（工業標準化法第 1 条)、同法が定める手続きに従って定められた各種製品の品質等の規格（JIS）に合致していると認められる製品に関し、当該製品の JIS への適合性を証明（認証）し、それを明示するために「JIS マーク」を製品や包装等に表示することを認める制度である。自社が提供する製品に JIS マーク表示に関することを希望する事業者が、国の登録を受けた民間の第三者認証機関から認証を受けることで、JIS マークの表示が可能となる（「新 JIS マーク表示制度について」http://www.jisc.go.jp/newjis/index.html ）。

工業標準化法は、「適正かつ合理的な工業標準の制定及び普及により工業標準化を促進する」ための法律であることから、同法によって、特定の事業者や製品に関し、認証マークの取得・表示を義務付ける等の規制は行っていない。にもかかわらず、広く JIS マークの表示（認証取得）が普及しているのは、同法が定める手続きに従って制定される規格に対する信頼性とマークの意義に関する認知度の高さにより、マーク表示を付すことが「市場における製品等の競争力となり得る」（製品等を提供する事業者がコストをかけて認証を得るインセンティブとして機能する。）という社会実態があるからであると考えられる。この信頼性と高い認知度が、同法が目的に掲げる「消費の合理化」（各製品の目的に照らし必要となる品質の要件（規格）を定め、それに従って、各製品を評価・比較するには、専門的な知識や評価のための環境等が必要になることから、個々の使用者・消費者が独自に各製品の品質を評価することは合理的でない。）を支えているものと考えられる。

3.1.2.2 消費生活用製品安全法等に基づく製品安全の制度

消費生活用製品安全法（昭和 48 年法律第 31 号）のように、一般消費者の生命又は身体に対する危害の防止を図るため、一定の製品を製造、販売する事業者に対し、製品に関する基準適合性についての認証取得およびその旨の表示を義務付け、その表示がない製品の製造、輸入又は販売を禁止する枠組みも存する。電気用品安全法（第 9 条：PSE 適合性検査)、ガス事業法（第 39 条の 11：特定ガス用品の適合性検査）等においても同様の枠組みが設けられている。また、家庭用品品質表示法は、適合性評価制度を定めるものではないが、同様の観点から、一定の製品に関し一定の表示を義務付けている。

消費生活用製品安全法による基準適合性評価・認証、表示義務の枠組みは、以下のように構成される。なお、同法に定める制度以外に、同法による適合性評価認証取得等の義務付けがない消費生活用製品をも対象として、財団法人製品安全協会が運用する民間の適合性評価制度（SG マーク制度）が設けられており、製品の利用に伴うリスクのレベルに応じ、多段階の評価・認証、表示制度が導入されている例として、参照に値するものであると考えられる。

特別特定製品（一般消費者の生命又は身体に対する危害の発生を防止するため必要な品質の確保が十分でない者がいると認められる特定製品（第２条３項）： 乳幼児用ベッド、携帯用レーザー応用装置、浴槽用温水循環器	主務大臣が一般消費者の生命又は身体に対する危害の発生を防止するため必要な技術上の基準を定める義務を負う（第３条)。	事業者は、事業者は、左の基準に適合するようにしなければならず、当該特別特定製品を販売する時までに、主務大臣の登録を受けた者による「適合性検査」を受け、かつ、交付を受けた証明書を保存しなければならない（第 12 条)。その義務を果たした場合に付すことが許される主務省令による表示（PSマーク）が付されているものでなければ、特定製品を販売、陳列できない（第 4 条)。
特定製品（消費生活用製品のうち、構造、材質、使用状況等からみて一般消費者の生命	同上	事業者は、左の基準に適合するようにしなければならず、その特定製品について検査を

又は身体に対して特に危害を及ぼすおそれが多いと認められる製品）（第２条２項）： 上記特別特定製品に指定されているもののほか、登山用ロープ、家庭用の圧力なべ及び圧力がま、乗車用ヘルメット		行い、その検査記録を作成し、これを保存しなければならない（第 11 条）（適合性検査は不要。財団法人製品安全協会が運用する民間の適合性評価制度である「SGマーク」の取得で代行可能）。かつ、PSマークが付されているものでなければ、販売、陳列できない（第４条）。
消費生活用製品（一般消費者の生活の用に供される製品）（第２条１項）	一部の製品について、財団法人製品安全協会が運用する民間の適合性評価制度である「SG マーク」制度により、基準の策定及び適合性認証制度が運用されている。	

3.1.3　情報セキュリティに関する第三者評価・認証制度

3.1.3.1 IT セキュリティ評価・認証制度

「IT セキュリティ評価及び認証制度」は、ISO/IEC15408 に基づく適合性評価制度である。製品やシステムが情報セキュリティの観点から適切に設計され、設計に基づく実装が漏れなくされているかどうかを認証機関とは別に認定される「評価機関」が基準に従って評価し、その評価結果を認証機関が検証して、基準に従って正しく「評価」」が行われたことを確認することができれば、認証書の発行を行う。

認証を取得する製品・システム開発者においては、基準に従ってセキュリティ機能の設計・実装を行うことにより、より安全な製品やシステムを提供することが可能となり、また、ユーザに対して製品の安全性を主張することが可能となる。本制度については、我が国が国際相互承認協定に認証書発行国のステイタスで加盟していることから、国内の制度によって得られた認証が認証書発行国および認証受入国においても同国の認証制度における認証書として通用するため、海外のユーザに対しても同様の主張を行うことが可能となる。

本制度における評価の範囲は、認証を申請する者が定めることとされており、その評価対象（TOE:　Target of Evaluation）のみについて評価・認証が行われることから、「製品」に関する評価・認証ではなく、製品のうちの「ある機能」に関する基準適合性を評価するものであるといえる。したがって、認証を取得したことを表示する場合には、製品全体についてセキュリティ機能が保証されているとの誤認を生まないよう適切な表示をするよう留意が求められる。

また、本適合性評価制度は、適合性の有無を Yes-No で評価する制度ではなく、レベル１から７に応じて、適切な評価保証レベル（EAL: Evaluation Assurance Level）を選択して評価を受けることができる。この場合の保証レベルは、セキュリティ機能のレベルをいうものではなく、評価の手続きのレベルをいうことに注意が必要となる（たとえば、レベル１は、設計仕様をマニュアルや機能仕様書の内容で確認し、レベル４は、ソースコードの実装レベルで仕様を確認する。）。

製品利用者においては、必要な保証レベルに応じたシステムを選択することが可能となるが、その一方で、自らが求めるセキュリティ機能が TOE となっている認証でなければ意味を成さないこととなる。

このように、認証を申請する者が評価を受ける対象範囲を定める適合性評価制度においては、評価の対象範囲を利用者側において正しく理解し、自らにとって必要となるセキュリティ仕様に合致するものかどうかを見極める能力が必要となる。

本制度は、ISO/IEC15408 及び国際相互承認協定（CCRA）に基づいて運用されているものであるが、国内法に具体的な根拠を有する制度ではない。制度発足を経済産業省が主導し、独立行政法人情報処理推進機構が認証機関となっていること、2013 年 3 月 31 日までの間、本認証制度に基づいて認証された OS などへの一定金額以上の投資について税制上の優遇措置が設けられていること（産業競争力のための情報基盤強化税制：http://www.meti.go.jp/policy/it_policy/zeisei/index.html#01）、情報セキュリティ政策会議において定められた「第 2 次情報セキュリティ基本計画」を受けて定められる政府「政府機関の情報セキュリティ対策のための統一基準第 4 版」において、

(g) 情報システムセキュリティ責任者は、構築する情報システムの構成要素については、重要なセキュリティ要件があると認めた場合には、当該要件に係るセキュリティ機能の設計に基づいて、製品として調達する機器及びソフトウェアに対して要求するセキュリティ機能を定め、当該

機能及びその他の要求条件を満たす採用候補製品が複数ある場合であって、その中に当該セキュリティ機能に関して IT セキュリティ評価及び認証制度に基づく認証を取得している製品がある場合には、当該製品を情報システムの構成要素として選択すること。(1.5.1.1. (g))

との記載が盛り込まれており、政府調達において認証製品の選択を推進すること、等により、制度の信頼性の向上、認証製品の増加を図り、民間における認証製品の普及を図るという推進施策が採られている。

3.1.3.2 暗号モジュール試験及び認証制度（JCMVP）

「暗号モジュール試験及び認証制度」は、「電子政府推奨暗号リスト等に記載されている暗号化機能、ハッシュ機能、署名機能等の承認されたセキュリティ機能を実装したハードウェア、ソフトウェア等から構成される暗号モジュールが、その内部に格納するセキュリティ機能並びに暗号鍵及びパスワード等の重要情報を適切に保護していること」について、試験（本制度では、評価（evaluation）ではなく試験（testing）が行われる。）及び認証を行う制度であり（http://www.ipa.go.jp/security/jcmvp/index.html)、ISO/IEC19790：2006（JIS X 19790:2007）（米 NIST 発行の FIPS140-2 が ISO/IEC 規格となったもの）に準拠するものである。

また、本制度は、上記「情報セキュリティ評価及び認証制度」と同様、国内法に根拠を有するものではないが、セキュリティ政策会議による「政府機関の情報セキュリティ対策のための統一基準（第 4 版)」において、

(g) 情報システムセキュリティ責任者は、暗号化又は電子署名の付与又は検証を行う必要があると認めた情報システムにおいて、選択したアルゴリズムがソフトウェア及びハードウェアへ適切に実装され、暗号化された情報の復号又は電子署名の付与に用いる鍵及び主体認証情報等が安全に保護された製品を使用するため、暗号モジュール試験及び認証制度に基づく認証を取得している製品を選択すること。(2.1.1.6.(g))

との記載が盛り込まれており、政府機関向けセキュリティシステムにおける調達を誘因に認証制度及び認証製品の普及を図る施策が進められている。

3.1.3.3 電子署名法に基づく特定電子認証業務の認定

我が国の電子署名法は、本人による一定の要件を満たした電子署名が付された電磁的記録に対し、手書きの署名や押印の付された文書と同等に、民事訴訟法上の文書の真正な成立の推定効（対象となる文書＝電磁的記録が署名者の意思に基づいて作成されたものであることの推定）を与えることを目的とするものである（第 3 条)。この場合における「一定の要件を満たした電子署名」とは、同条において、「電子署名を行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるもの」とされており、この要件は、「特定認証業務」の対象となる電子署名の定義と一致させられてある（「この法律において「特定認証業務」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。」）ことから、「特定認証業務」の対象となる電子署名は、文書の真正な成立の推定効を付与されるものとして評価される、という構成が採られている（同法第 2 条第 3 項)。

「特定認証業務」の認定基準は、同法第 3 章第 1 節及び同法施行規則に定められており、申請のあった認証業務が同基準に適合するものであるかどうかを国（主務大臣）に代わって調査する機関として指定調査機関が指定されることとされている（同法第 17 条)。

認証業務そのものは、上述のとおり、電子署名に用いられる署名(秘密)鍵に対応する検証（公開）鍵が特定の者に関係づけられることを証明する業務を言うものと定義づけられており（同法第２条第２項)、規格・基準への適合性ではなく、電子署名の作成者の確認のために用いられる公開鍵とその公開鍵で検証される秘密鍵が帰属する個人との結びつきの確からしさを証明するもの、すなわち申請に係る公開鍵に関する証明書を請求する利用者が、当該公開鍵に対応する秘密鍵を有していること、及び、当該証明書に記録する利用者の表記が証明書を請求する利用者に関する記載に相違ないこと（請求者の本人確認）という事実を確認・証明するものである。したがって、一定の事実を第三者が証明するという観点では第三者認証制度であることに間違いはないが、第三者が規格・基準への適合性を評価するという観点で捉えると、その認証業務が特定認証業務であることを認定する指定調査機関における業務のほうが、近しいといえる。

3.1.3.4　情報セキュリティマネジメントシステム適合性評価制度

情報セキュリティに関するガバナンスの問題に最も影響のある第三者評価認証制度であると考えられる。詳細については、本章 4 で記述されるが、本項においては、本適合性評価制度と情報セキュリティ監査との違いを整理する。

情報セキュリティマネジメントシステム適合性評価制度（ISMS 適合性評価制度）と情報セキュリティ監査は、いずれも独立の立場の第三者が対象組織において情報セキュリティ対策が有効に機能しているかについて評価を行うものであるが、ISMS 適合性評価制度においては、評価・認証を受ける対象範囲は認証を依頼する組織において設定可能であるものの、評価の基準は、JISQ27001：2006 の要求事項であって、この基準自体は認証を受ける側において修正・変更を行うことができない。一方で、情報セキュリティ監査は、監査依頼者において設定し、状況に応じて監査項目を調整した「個別管理基準」を利用することが可能とされている。また、ISMS 適合性評価制度における認証機関は、基準に従って認定を受けた審査登録機関でなければならないが、情報セキュリティ監査制度においては、監査人の選定に関する規格は定められておらず、一般には、情報セキュリテイ監査企業台帳や、JASA の公認情報セキュリティ監査人資格制度が利用されている。

3.1.3.5 事業継続マネジメントシステム適合性評価制度(実証運用＝正式運用に向けての準備中)

近年、我が国では大規模地震等の自然災害を中心に、欧米ではテロの脅威を念頭において、事業継続に対する関心が高まりつつある。事業継続を巡る国際標準化の動きも急速である。2006 年 11 月には、英国規格協会（BSI：British Standards Institution）が BCM のガイドラインとなる「BS25999-1：事業継続管理-第 1 部 実践規範」1 を発行、国際標準化機構（ISO：International Organization for Standardization）に提案するとともに、翌年 11 月には BCMS（事業継続マネジメントシステム）に関する認証基準となる「BS25999-2：事業継続管理-第 2 部 仕様」を発行、第三者認証の取り組みも始まっている。また、ISO では、社会セキュリティに関する標準化を行う専門委員会 TC223 の総会（2008 年 5 月）において、事業継続マネジメントに関する公開仕様書「PAS 22399：社会セキュリティー緊急事態準備と業務継続マネジメントガイド」の IS（国際規格）化、及び要求事項規格の開発を行う WG4 の設置が決定した。

英国規格協会（BSI）が策定した BS25999-1「事業継続管理」では、BCP は、「組織が予め定めた許容可能なレベルで、その重要な活動を実施し続けることを可能とするため、何らかのインシデント発生時に備え、開発され、まとめられ維持されている文書化された一連の手順および情報の集合体」と定義されており、BCM は、「組織への潜在的脅威や、そうした脅威が現実となった場合に引き起こされる可能性のある事業運営上の影響を特定する包括的なマネジメントプロセス」と定義されている。

BCM のライフサイクルが効果的に運用管理され、改善されることを確実にするマネジメントシステムが BCMS(事業継続マネジメントシステム)であり、前述の BS25999-2 によると「マネジメントシステムぜんたいの中で、事業継続の確立、導入、運用、監視、レビュー、維持及び改善を担う部分」と定義されている。

この事業継続マネジメントシステムに関し、組織（企業等）のマネジメントシステムが規格に適合しているかどうかを第三者が評価する適合性評価制度の実証運用が、財団法人日本情報処理開発協会において、平成 20 年度から開始されている。実証運用時においては、適合性評価の対象となる認証基準は、BS25999-2 とされており、実証運用を通じて正式運用時のBCMS認証基準の内容も検討することとされている（財団法人日本情報処理開発協会情報マネジメントシステム推進センター　BCMS 適合性評価制度（実証運用）のページ参照。http://www.isms.jipdec.jp/bcms/bcms_seido.pdf)。

3.1.3.6 プライバシーマーク制度

「プライバシーマーク制度」については、次頁以降において詳述される。

4　プライバシーマーク制度とその問題点

4.1　制度の目的

4.1.1　JIPDEC の掲げる制度目的

財団法人日本情報処理開発協会(Japan Information Processing Development Corporation, JIPDEC)は、プライバシーマーク制度の目的として、次の２つをあげている（JIPDEC ホームページ参照)。

①　消費者の目に見えるプライバシーマークで示すことによって、個人情報の保護に関する消費者の意識の向上を図ること
②　適切な個人情報の取扱いを推進することによって、消費者の個人情報の保護意識の高まりにこたえ、社会的な信用を得るためのインセンティブを事業者に与えること

プライバシーマークが目に止まれば、人間の目に見えることは確かであるが、そのことがなぜ消費者の意識の向上につながるのか、いまひとつ理解し難いように思われる。制度目的が不明確であるということは、現在のプライバシーマーク制度が何を目指し、何のために認証制度を行っているのかについて、十分なコンセンサスが形成されていないという誤解を与えかねない。社会的な理解を得ていくためにもより明確な制度目的を示すべきである。

4.1.2　制度目的の再確認

ここでは、プライバシーマーク制度の目的を再確認しておくことにしたい。

①　消費者保護
　－消費者がマーク表示の有無を確認することによって、事業者の個人情報の取扱いに関する安全性の有無を簡易に判断できるようにすること

消費者等本人は、ある事業者と契約の締結に伴い個人情報を提供したり、あるいはアンケート調査に応じたり、懸賞へ応募したりするなど個人情報を提供することがあるが、そうした場合は、相手方事業者の個人情報保護の管理システムが一定レベルに達しているのかどうかを確認し、自ら注意しなければならない。しかし、一消費者がそれを行うことは実際上容易ではない。本制度は、消費者等本人に対して、このことを簡単に確認することができるよう専門家が審査し、合格事業者にマークを付与することで、誰でも簡便に事業者の評価を行えるようにしている。

②　事業者の自主規制の推進
　－事業者に対して、個人情報保護体制整備へのインセンティブを創出すること

付与認定を受けた事業者は、プライバシーマークを消費者や委託元、その他の取引先等に示すことで、自社の個人情報保護体制が JIS Q 15001 に適合したものであることをアピールでき、一定の社会的信用を得ることができる。

③　社会的な意義
　日本の事業者及び社会の個人情報保護の水準の底上げを図ること

JIS Q 15001 への適合事業者を増やしていくことは、日本国内の事業者の個人情報保護の水準を底上げすることに寄与する制度といっていいだろう。

個人情報保護法は、「個人情報取扱事業者」の個人情報（個人データ、保有個人データ）の取扱いに関する最小限の基準（ミニマム・スタンダード）を示して、その遵守を法的に義務付けている。一方、JIS Q 15001 は、より広く「事業者」一般の個人情報（特定の機微な個人情報、開示対象個人情報）の取扱いのルールを定めることで、法令等を遵守するための管理の仕組み（マネジメントシステム）や手順を要求事項として示す役割を担っている。

プライバシーマーク制度は、その運営を通じて、抽象的な JIS Q 15001 の要求事項を審査基準という形で具体化し、審査を通じて、また、各事業者が JIS Q 15001 等を活用しよりよい管理システムが構築できるよう情報提供していくことで、適正な経営管理を促し、社会全体の個人情報の保護の水準を高めていくことが期待されている。

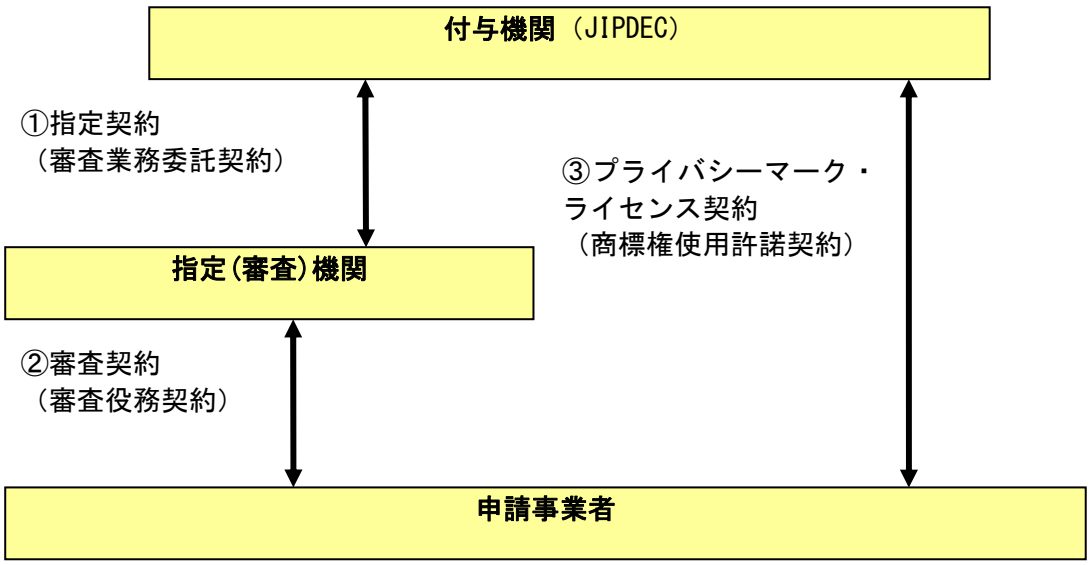
4.2　プライバシーマークの問題点

4.2.1　制度の法的構成

プライバシーマーク制度は、政府認証ではなく、あくまでも民間認証制度である。したがって、その制度の根拠は、法律によるものではなく、対等な私人間の契約によって構成されなければならない。

まず、審査制度の主体に関する規程が必要であろう。プライバシーマーク制度においては、制度を主宰する付与機関、及びプライバシーマークの付与のための審査を行う指定（審査）機関の組織規程を定めている。

次に、審査主体の権限、審査基準、審査手続、不利益措置の基準等を定めるために必要な契約が必要となる。プライバシーマーク制度は、下図のように①指定契約、②審査契約、③プライバシーマーク使用許諾（ライセンス）契約の３つの契約関係で構成している。これらの基本的な枠組みは、運営要領に定められることになっている。要するに運営要領は契約（約款）としての性質を有している。



①　指定契約（審査業務委託契約）

指定契約とは、付与機関（JIPDEC）と指定機関（の申請団体）との間で締結される審査業務の委託契約のことをいう（運営要領第５条第２項）。[15]

指定機関にとっては指定機関としての地位の根拠となる契約であり、付与機関（JIPDEC）においては指定機関を監督、指導する根拠となる契約である。付与機関は、指定機関において契約違反の事実がある場合は、指定機関契約の解除事由に該当するか否かを判断する。場合によっては、本契約に基づき、指定機関の取消（指定契約の解除）をすることで制度の信頼性を維持しなければならない。

②　審査契約（審査役務契約）

審査契約とは、指定機関と申請事業者との間のプライバシーマーク審査に関する役務契約のことをいう。申請が「申込み」となり、かかる申請書類の受理を「承諾」として契約が成立するという構成である。審査料は、審査役務の対価ということができる。

なお、指定（審査）機関は、受理するに際して、申請書類の形式的確認と欠格事由の有無などの審査を行う。

ここでの欠格事由として、ａ）反社会的勢力の排除（取締役等の懲役禁固刑だけの欠格事由で十分に排除できるか）、ｂ）欺瞞的な消費者取引を行っている事業者の排除（JIS Q 15001 に準拠したマネジメントシステムのみを見て認証マークを付与するのが適切か制度目的との関係が問われる。）、ｃ）十分な経営上の資力（信用）がない事業者の排除（倒産と個人情報の散逸リスクをどのように評価するかが問われる。）などをどのように扱うか、欠格事由の定め方に課題が残って

[15] 運営要領第５条第２項は「指定機関は、この要領及び第 26 条第２項の指定機関の指定に関する契約に定めるところに従い、第２章から第４章までの規定により指定機関が行うものとされたプライバシーマーク付与認定に係る業務（以下「指定業務」という。）を行う。」と定めている。

いる。

③　プライバシーマーク・ライセンス契約（商標権使用許諾契約）

プライバシーマーク・ライセンス（商標権使用許諾）契約とは、付与機関（JIPDEC）が、審査契約に基づき、個人情報保護マネジメントシステムの JIS Q 15001 適合性を評価（審査）の結果、適合性ありと認められた事業者に対し、プライバシーマークの使用を許諾する契約のことをいう。

付与機関（JIPDEC）は、再度、上述した欠格事由に該当していないことを確認した上で、指定機関の審査を合格した事業者との間でプライバシーマーク（商標権）の使用許諾（ライセンス）契約を締結する。使用許諾に関する条件は、主に「運営要領」に明記されている。単なる商標権使用許諾契約ではなく、JIS Q 15001 へ適合した運用をその許諾の条件とし、報告義務、調査に応じる義務などの権限が付与機関や指定機関にあることを契約の条項に明記することになる。

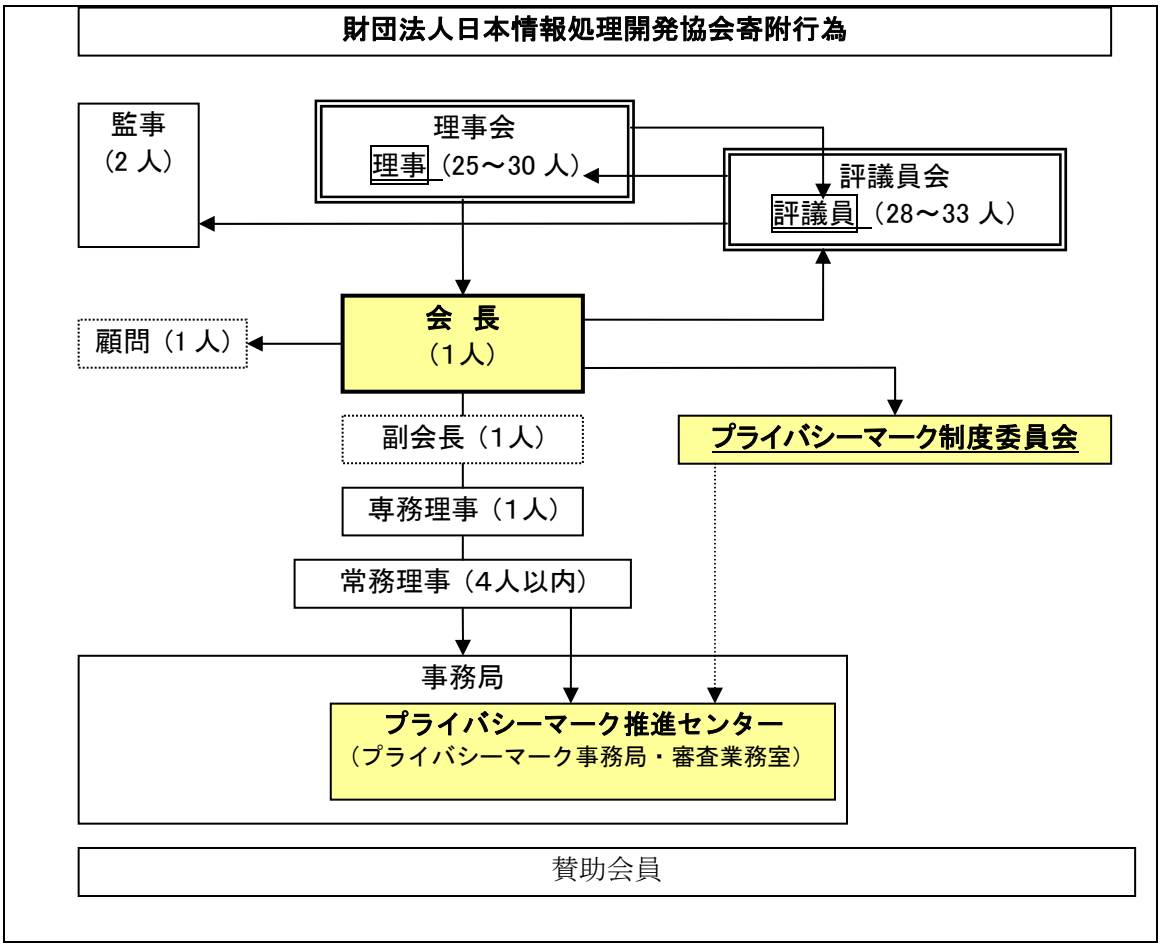
政府認証制度においては、法律に根拠を持つこうした権限は、民間認証制度においては、契約における債権として契約内容に盛り込まれなければならず、当然ながら、契約に基づかない中での相手方への優越的な立場からの要請は、原則として許されるものではない。

特に、プライバシーマークの取消は、契約の解除という性質を有しており、契約の根拠なく一方的に解除することはできず、取消の基準は契約の解除事由として明確に定める必要がある。また、契約の解除に至らないその他の不利益措置についても、同様に明記するとともに、その決定過程の透明性と公平性の確保、手続規定の整備は、公益を目的とする民間認証制度においては、非常に重要である。

4.2.2　制度の運営主体と構造的な問題

プライバシーマーク制度の運営主体である JIPDEC は、通商産業大臣（現経済産業大臣）及び郵政大臣（現総務大臣）によって認可され、昭和 42 年 12 月 20 日に設立された公益法人であり、基金は、39 億 9、900 万円、年間予算は 50 億円前後、職員数は約 150 名という規模の組織である。経済産業省・総務省共管の団体であるが、会長が経済産業省の事務次官経験者から選任されてきたように、一般に経済産業省所管の公益法人として理解されている。

しかし、その運営するプライバシーマーク制度に対しては、構造的な問題を指摘せざるを得ない。



1　組織規程の未整備

JIPDEC の組織は、上図のとおりであるが、まず、組織規定の未整備を指摘したい。JIPDEC の事務局に当たるプライバシーマーク推進センターは、「プライバシーマーク事務局」と「審査業務室」の２つの部署で構成されている。また、プライバシー事務局内には「相談窓口」も設置されている。しかし、「プライバシーマーク推進センター」は、運営要領上の組織ではない。設置の根拠は、JIPDEC 内部の組織規程によるものと思われる。要するに、プライバシーマーク制度における機関の根拠規定を運営要領上に全て置くかどうかという点が曖昧なまま運営されている。同様に「事務局長」（運営要領 42 条 3 項）は、運営要領上の役職であるが、プライバシーマーク推進センターのセンター長、副センター長は運営要領上の役職ではなく、事務局長との指揮命令関係など、その位置づけは、外部から不透明である。（現在は、センター長が事務局長を兼務するかたちで人事上、こうした矛盾は回避されている。）組織規程の未整備は、本制度の課題の１つであるといわなくてはならない。

2　指定機関と付与機関の併存

運営要領では、付与機関（JIPDEC）にプライバシーマーク事務局を置くことが定められている（40 条 1 項）。プライバシーマーク事務局は、プライバシーマーク制度の企画立案及び運用並びに普及に関する事務を担当している（同条 2 項）。なお、プライバシーマーク事務局に事務局長を置くものとしている（同条 3 項）。

審査業務室は、どの指定機関にも属していない事業者等からの申請を受け付けるため、プライバシーマークの審査業務等指定業務を担当している（運営要領 35 条）。改善措置及び付与契約の解除も行う（同 36 条）。審査業務室は、指定機関の業務（指定業務）を行う組織である。しかし、これは付与機関としての本来的業務ではない。指定機関の審査のあり方を監督すべき付与機関が、自身で審査を行うのは、その公平性、客観性の観点から第三者評価認証制度のあり方としては明らかに問題がある。また、同一法人内では指定契約の締結もできない。

これは、制度創設当初、指定機関が JISA のみであり、JISA 会員以外の申請を受け付ける必要があったことから、暫定的にとられた措置であった。制度創設 10 年以上を経て、10 を超える指

定機関を指定した今日においては、早期に廃止に向けた準備を開始する必要がある。

また、暫定的であれ、審査業務を行うのであれば、最低限、運営要領を改正し、指定機関と同等の監督に服するよう見直すべきである。すなわち、a)指定機関としての実質的要件を充足すること（外部有識者を中心とした審査会など独立した合否の「意思決定機関」を設置すること）、b)プライバシーマーク事務局（審査の監督機関）と審査業務室（指定機関）との組織間の障壁を厳格に設けること、c)プライバシーマーク事務局（審査の監督機関）と審査業務室（指定機関）を厳格に監査するとともに、その結果を公表することなどの対応が必要である。

3　組織体制の不備

運営要領は、付与機関（JIPDEC）にプライバシーマーク制度委員会を置くことを義務づけている（37 条）。

プライバシーマーク制度委員会の委員は、個人情報の取扱い及び保護に関し学識経験がある者の中から JIPDEC 会長が委嘱し（39 条 1 項）、委員の互選により委員長を選任する（39 条 2 項）。プライバシーマーク制度委員会の事務は、プライバシーマーク事務局が行うことになっている（39 条 3 項）。

プライバシーマーク制度委員会は、運営要領に規定する次の事項のほか、プライバシーマーク制度の企画立案及び運用に関する重要事項について審議する（38 条）。しかし、決定権はなく、あくまで審議し答申するに止まる。

指定機関が決定する次の事項については、運営要領上、プライバシーマーク制度の審議の前置が義務付けられている。

① 合併又は分社化によるプライバシーマーク使用許諾契約上の地位の存続・承継に関する決定と決定手続の審議（運営要領 15 条 2 項前段及び 3 項）
② 注意、勧告の決定に際しての審議前置（同 21 条 2 項）
③ 認定の一時停止の決定に際しての審議前置（21 条の 2、1 項、2 項）
④ 認定の取消しの決定に際しての審議前置（22 条 1 項、2 項）

付与機関が決定する次の事項については、運営要領上、プライバシーマーク制度の審議の前置が義務付けられている。

① 指定機関の指定（運営要領 26 条 1 項）。
② 指定契約の更新可否の決定（30 条 3 項）。
③ 指定機関に対する勧告又は要請（32 条）
④ 指定の取消し（33 条 1 項）
⑤ 改善措置及び付与契約の解除（20 条～21 条の 2、36 条 1 項）

ここで、注意しなくてはならないのは、「プライバシーマーク制度委員会」が、JIPDEC 会長のいわゆる諮問機関的性格しか与えられていないということである。運営要領上、会長は、各種の重要事項に関して、「プライバシーマーク制度委員会」の審議の結果と異なる決定をすることが可能であるということである。また、プライバシーマーク制度委員会の審議の前置を運営要領に明記しているもの以外は、当然ながら審議することなく会長が決定できる。

要するに、運営要領上は、会長を単独の意思決定機関とする第三者評価認証制度となっているということが特徴である。JISA などの指定機関においては、団体の会長や理事会とは独立した「審査会」を組織し、外部有識者を指名して審査合否や不利益措置に関する意思決定機関としているところと異なった体制にある。JISA の仕組みがプライバシーマーク制度の本来的姿であろう。

また、プライバシーマーク事務局の職員は、会長、副会長、専務理事、及び常務理事の指揮命令の下にあり、プライバシーマーク制度委員会の下にあるわけではなく、審査員も同様である。

こうした組織体制が第三者評価認証制度として正しいあり方であるかどうか、独立性、公平性、透明性、専門性という観点から点検することが必要である。少なくとも、ア）プライバシーマーク制度の設計、イ）プライバシーマークの認定付与、ウ）取消し等不利益措置の決定といった重要事項については、外部有識者に委嘱した合議制の意思決定機関が必要であり、運営要領上もその点を踏まえて、抜本的な改正に着手しなくてはならない。

もし、現在の組織体制のままでいくとするのであれば、JIPDEC 会長を単独の意思決定機関とする第三者評価認証制度となっていることを宣言するなど、意思決定機関の所在をもう少しわかりやすく外部に示すべきである。

4　指定機関のばらつき

プライバシーマーク付与認定指定機関（指定機関）とは、運営要領に基づき、付与機関である JIPDEC との指定契約において指定された団体をいう。しかし、付与機関においては、「プライバシーマーク付与指定機関指定基準」が用意されているようであるが、その内容は公表されていない。

指定機関ごとに審査会の名称、委員の要件、法的な位置づけ、その権限の内容が異なる。審査会の審査のあり方も統一されていない。申請事業者との守秘契約も指定機関ごとに委ねられるなど、プライバシーマーク制度としての最低限の統一性に欠けるところが散見される。審査会は、弁護士等法律家、情報セキュリティ等の技術者、経営者等経営管理の知識と実務経験のある者など過半数の外部有識者に委員等を委嘱すべきである。少なくとも、JIPDEC においては、創設より過去 10 年間、審査会を設置せず、事務局内だけで実質的な認証を行ってきており、指定機関に対してのみ、審査会を設置するよう求めることができなかった。JIPDEC 自身が指定機関を兼ねていること、指定機関指定基準が内規としてのみ存在し、詳細を外部に公開しないこと、またはその体質を含めて課題が残っている。

5　費用の適正さの検証と会計監査の必要性

審査基準の詳細化とあいまって、審査報告書への詳細な記述が求められるなど審査員の負担も増加している。審査の詳細化が健全な審査へとつながるものであればともかく、一定時間内の審査項目が増加することのしわ寄せは、審査範囲の限定化によって帳尻をあわせることにもつながりかねない。プライバシーマーク制度の場合は、審査と補正のやりとりが続き、事実上審査時間が延長されているところもあり過度な審査料を請求しているとの批判は当たらないところもあるほか、指定機関によっては審査業務にかかる費用が一部持ち出しになる例もあるように聞いている。

しかし、JIPDEC におけるプライバシーマーク制度の付与機関としてのマーク使用料は、年間 50,000 円～200,000 円×約１万社÷２年分の収入となり、それに指定機関としての申請料及び審査料収入が追加されることになる。その総額はかなりの金額となる。制度単体の収支の報告は当然必要であり、ある程度は JIPDEC として行われているであろうが、その結果は、取得事業者や申請予定の事業者など利害関係人に対しても広く公開されるべきであり、また制度単体の監査報告書なども公開されることが望ましいのは当然である。こうした情報公開があって、はじめて費用の適正さの検証が可能となるからである。このことは漢字検定協会の不祥事を見るまでもなく明らかであり、過度な NPO ビジネスと化さないような仕組みづくりも求められているというべきである。

6　不透明な不利益措置（注意、勧告、一時停止、取消し）

不利益措置は、指定機関が、プライバシーマーク付与認定を受けた事業者に対して行う。

不利益措置の基準は、運営要領によれば、「この要領に基づき別に定める基準」に従うこととされている。しかし、指定機関で用いられている当該基準については公表されておらず指定機関に対しては当該文書を対外秘とするよう指導されているのが実態である。また、「欠格レベル」という用語にもみられるように、プライバシーマークの申請を受理するかどうか（契約の申込みに対して承諾するかどうか）に際しての申請事業者の資格を問う「欠格事由」と、プライバシーマーク取得後の取消事由（プライバシーマークの使用許諾契約の解除事由の意味となる。）及びその他の不利益措置の区別を十分に理解していないように見受けられる。また、「欠格レベル」がどのように区分されるのかの基準も公開されていない。発生した事象と原因によりポイント制で基準値を定め 10 段階に区分して、不利益措置を決めるというものであるが、法的な説明に耐えられる考え方であるか、非公表では検証の機会もなく、異議を申し述べる機会も事実上奪われた状態である。この基準は誰がそのような考え方の下で起案しどのような手続きで承認され、何故それに契約上の拘束されなければならないのかが明らかにされなければならない。

マークの取消等不利益措置の基準が十分に公開されていないことは、プライバシーマーク制度の重大な欠陥の一つであると言わざるをえない。取消などの措置がなされ公表された場合は、株価をはじめとする企業評価にも影響を与えかねない重大な問題である。

正しい基準は、そのすべてを公表できるものであり、公表することによって正しいメッセージが取得事業者と社会に伝わり、事業者の違反の抑止と改善の契機となるものである。それを秘匿することにこだわる JIPDEC の姿勢は批判されて当然といわなくてはならない。

以上の問題点を踏まえ、第 4 編において、民間認証制度に求められる諸原則を提言する。

5　ISMS 適合性評価制度とその問題点～外部委託を中心に～

5.1　ISMS 適合性評価制度とは

企業における情報セキュリティガバナンスを実効あらしめる仕組みとして、現在、最も普及している第三者認証制度に、情報セキュリティマネジメントシステム(Information Security Management System, ISMS)適合性評価制度がある。これは、評価機関が、企業の ISMS を評価し、国際標準規格である ISO/IEC27001:2005 に準拠していると認証した場合に、その事業者に対して、適合性を証するシール(マーク)を付与し、これを表示することを認める制度である。JIPDEC が主体となって行っている制度であり、本格運用は 2002 年 4 月から開始された。

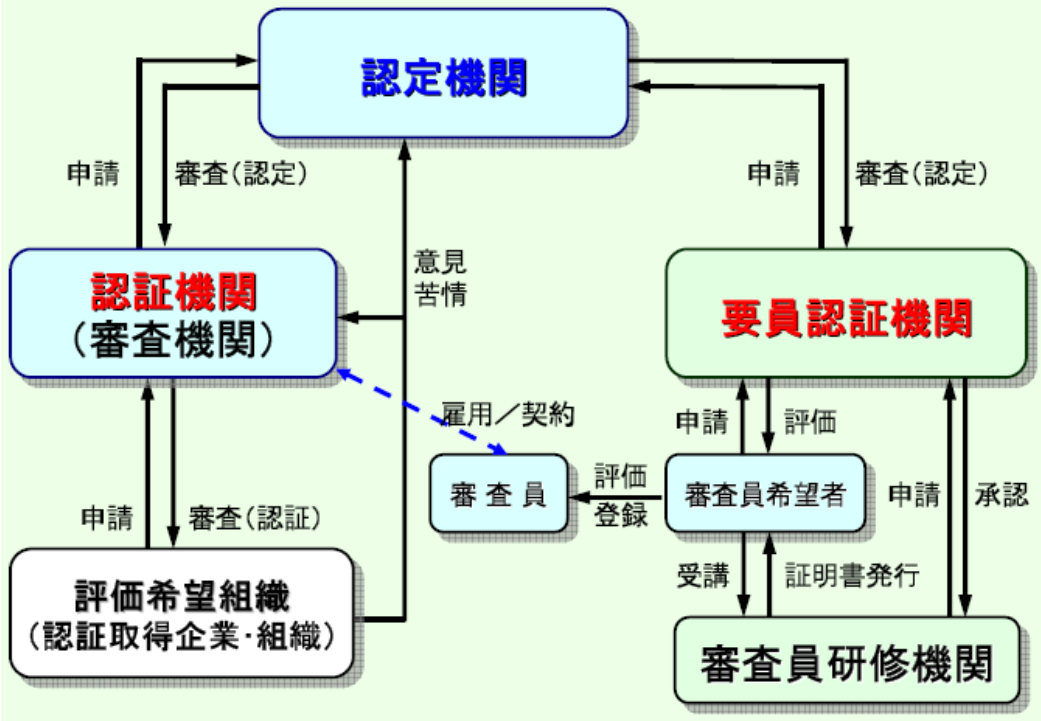
ISO/IEC 27001:2005 は、英国標準規格 BS7799 がもととなっている。同規格は、1998 年に二部構成に分けられ、Part1 は情報セキュリティマネジメントを実践するための規範、Part2 は情報セキュリティマネジメントの認証に用いるための規格である。

Part1 は、2000 年に ISO/IEC 17799:2000 として国際規格化され、さらに日本工業規格としてローカライズされた JISX5080:2002 が 2002 年に制定された。ISO/IEC17799:2000 は 2005 年 6 月に ISO/IEC17799:2005 へと改訂された。本改訂に対応する日本工業規格はその技術内容及び構成を変更することなく、ISO/IEC27000 シリーズ化に伴う番号変更計画を先取りして、JISQ27002:2006 として 2006 年 5 月に制定された。これによって JISX5080 は廃止された。

Part2 は、情報セキュリティマネジメントの認証に用いるための英国規格として位置づけられている。2002 年の改訂版を経て、2005 年 10 月に、ISO/IEC27001:2005 として国際規格化された。わが国においても、その技術内容及び構成を変更することなく、2006 年 5 月に JISQ27001:2006 として国内規格化された。ISMS 認証取得事業者数は、世界の中でも日本だけが突出して多く、2009 年 10 月 23 日時点で、3300 件を越えている。

5.2　ISMS　適合性評価制度の運用

ISMS 適合性評価制度の基本的な運用の仕組みは、以下の図に示すとおりである。



情報マネジメントシステム推進センター「情報セキュリティマネジメントシステム(ISMS)適合性評価制度の概要」(http://www.isms.jipdec.jp/about/index.html)より。

ISMS 適合性評価制度は、組織が構築した ISMS が JIS Q 27001 (ISO/IEC 27001) に適合しているか否かを審査し登録する「認証機関」、審査員の資格を付与する「要員認証機関」、及びこれら各機関がその業務を行う能力を備えているかをみる「認定機関」から構成される。

なお、審査員になるために必要な研修を実施する「審査員研修機関」は要員認証機関が承認する。

ISMS の場合は、JIPDEC は認定機関であり、実際に審査を行うのは認証機関である。

2009 年の 10 月 19 日現在で、26 の認証機関が認定を受けている。P マークの場合は、JIPDEC が指定機関(ISMS でいうと認証機関に相当)との間で審査業務委託契約を結ぶが、ISMS の場合は、認証機関となりたい事業者が申請を行って認定を受けるというもので、契約は締結されないとのことである。

評価を希望する組織は、一覧の中から申請する対象の認証機関を選択し、両者の間で、見積もりを経た後、認証契約を締結する。認証機関は、書類審査、実地審査を経て、問題がなければ認証登録を行い、評価希望組織に対し、登録書を発行して ISMS マークを付与する。認証の有効期間は 3 年間である。認証を維持するためには、1 年未満のサイクルで維持審査を実施し、3 年以降も認証を継続する場合は、更新審査が行われる。

ISMS で用いられるマークには、JIPDEC が認証機関に使用させるマークと、認証機関が評価を受けた組織に使用させるマークがある。JIPDEC のマークは商標登録が行われており、使用規程に基づき運用されている。認証機関は、JIPDEC のマークに加え、認証機関独自のマークを用いて、対象事業者に付与するという形を取る。P マークの場合は、JIPDEC と認証を受けた事業者との間で個別に商標使用契約を結ぶが、ISMS の場合は、認証機関に対して使用規程に則って運用するようにとの指示を出し、認証機関がそれに従ってマークを使用するという処理がなされている。

5.3 ISMS 適合性評価制度の要求事項

ISO/IEC27001:2005(JISQ27001:2006)は、冒頭の 0.を入れると、9 つのセクション及び 3 つの付属書で構成されている。本規格は、主として認証取得のために用いられるものである。

また、本規格は、ISO9000 や 14000 シリーズと同様に、PDCA モデルによるマネジメントシステムを採用している。

PDCA サイクルとは、P(Plan-計画)、D(Do-実行)、C(Check-点検)、A(Act-処置)を繰り返すことによって、目標となる事項の継続的な水準の維持・向上を図ろうとするものをいう。

ISO/IEC27001:2005 要求事項の概要

番号	項目名	番号	項目名
0.1	序文	4.3.2	文書管理
0.2	ISMS の採用	4.3.3	記録の管理
0.2.1	概要	5	経営陣の責任
0.2.2	プロセスアプローチ	5.1	経営陣のコミットメント
0.2.3	他のマネジメントシステムとの両立性	5.2	経営資源の運用管理
1	適用範囲	5.2.1	経営資源の提供
1.1	一般	5.2.2	教育、訓練、意識向上及び力量
1.2	適用	6	ISMS 内部監査
2	引用規格	7	ISMS へのマネジメントレビュー
3	用語および定義	7.1	一般
4	情報セキュリティマネジメントシステム	7.2	レビューへのインプット
4.1	一般要求事項	7.3	レビューからのアウトプット
4.2	ISMS の確立及び運営管理	8	ISMS の改善
4.2.1	ISMS の確立	8.1	継続的改善
4.2.2	ISMS の導入及び運用	8.2	是正処置
4.2.3	ISMS の監視及びレビュー	8.3	予防処置
4.2.4	ISMS の維持及び改善	附属書 A(規定)	
4.3	文書化に関する要求事項	附属書 B(参考)	
4.3.1	一般	附属書 C(参考)	

岡村久道『情報セキュリティの法律』(商事法務、2007 年) 256 頁の表 20 より

また、リスク対応の際に選択肢となる管理策は、この規格の附属書 A が規定しており、11 のセクションと 133 の管理策から構成されている。なお、附属書には、管理目的及び管理策のすべては網羅されていないので、組織は、管理目的及び管理策の追加が必要であると考えてよい旨が記されている。したがって、組織は、追加的に、情報の機密性を保護するためという管理目的で、私物パソコンの職場持込み禁止等の管理策を選択することとなる。

具体的には、「A.5　セキュリティ基本方針」、「A.6　情報セキュリティのための組織」、「A.7 資産の管理」、「A.8　人的資源のセキュリティ」、「A.9　物理的及び環境的セキュリティ」、「A.10 通信及び運用管理」、「A.11　アクセス制御」、「A.12　情報システムの取得、開発及び保守」、「A.13 情報セキュリティインシデントの管理」、「A.14　事業継続管理」、「A.15　順守」で構成されている[16]。

5.4　外部委託における ISMS 認証制度の活用

今日の組織における業務を考えるときには、組織の業務の一部を外部委託（組織外に業務を委託）することを前提に考える必要がある。そのとき、業務委託先における情報セキュリティ対策実施状況の適正性について第三者による適合性評価制度を活用するには、その活用方法についてリスクマネジメントの視点で再確認することが重要である。特に、マネジメントシステムに関する適合性評価制度の場合には注意が必要である。その代表的な制度として、ISMS適合性評価制度[17]について説明する。マネジメントシステムに関する同様の制度として、他にプライバシーマーク制度[18]があるが、差異がある箇所については、その旨の説明を加える。

ISMS は情報セキュリティマネジメントシステムの略であり、語法としては、「組織が ISMS を構築する」などのように使う。一方で、ISMS 認証は、ISMS 構築についての第三者による適合性評価制度により認定される認証のことであり、語法としては、「組織が ISMS 認証を取得する」というように使う。ISMS は、情報セキュリティに関するマネジメントシステムの考え方の総称であるのに対して、ISMS 認証は、国際規格である ISO/IEC 27001 に基づいたもので、その国内規格として JIS Q 27001 に基づいた具体的なものである。組織における ISMS 構築は、ISMS 認証の考え方に限られるものではないが、国内では、ISMS 認証の認定を受けていることが ISMS であるかのように誤解している場合もある。

したがって、組織が ISMS を構築することは、ISMS 認証の規格には本来限られるものではないが、ここでは最終的に ISMS 認証の活用方法について考察するため、マネジメントシステムとして、ISO/IEC 27001 に基づいた ISMS 構築を前提として説明をする。

5.5. 外部委託の種類

外部委託については、委託する業務の内容によって一様に整理できるものではないが、概ね２つに分けて考える。１つには、定型のサービスとして提供されているサービスを利用するものであり、もう１つは業務内容を仕様として指示して委託するものである。前者の例として、宅配業者やネットワーク通信プロバイダ業者などがあり、委託先となる事業者が予め定めた共通のサービス仕様や約款に基づいてそのサービスを発注して委託する。後者の例として、システムインテグレーション業務やアプリケーションソフトウェア開発業務などがあり、委託する業務の内容は委託元が発注ごとに仕様書などで指定して委託する。

以降の説明では、後者にあげた、業務内容を仕様として指示して委託する業務について取り上げて説明する。

5.6　マネジメントシステムに係る認証制度

5.6.1　対策のマネジメントシステムと対策のレベルの違い

ISMS 認証及びプライバシーマークは、それぞれ、情報セキュリティ対策及び個人情報保護対策のマネジメントシステムについての認証制度である。これらが、対策レベルの認証ではなく、対策のマネジメントシステムに係るものであることについて正しく理解することが重要である。

マネジメントシステムの構築では、リスクの分析・評価とその対応が求められる。リスクの分

---

16 岡村・前掲『情報セキュリティの法律』268～270 頁

17 ISMS 適合性評価制度：http://www.isms.jipdec.jp/.

18 プライバシーマーク制度：http://privacymark.jp/

析・評価とは、存在するリスクを分析し、それへの何らかの対策の結果残る残存リスクについて評価することである。評価結果に基づいて、そのリスクへの対応の選択肢の一つとして、残存リスクを組織として許容するかどうかを決定する。別の選択肢として、そのリスクを許容せずに回避することを決定した場合には、一般的には、そのリスクが生じる原因となる何らかの組織活動を制限又は禁止することになる。

残存リスクの許容レベルが決定することにより、対策で求められる要求レベルが決まる。対策の要求レベルが決まると、それを達成するために必要な対策方法が決まることになる。一般的には対策の要求レベルを満たすことができれば、対策方法の選択については柔軟性が認められることになるが、対策方法が同一ではないことが管理上のリスクと考えられるなど何らかの支障があれば、対策方法が画一的なものとなる。

以上のような段階的な決定がなされ、対策が立案され、実施される。そして、その実施内容が検査され、検査結果に基づいて立案されたとおりに実施されていなければ、リスク分析・評価又はその対応、それに基づく対策立案内容、さらにそれに基づく実施内容のいずれかを是正するというマネジメントサイクルによって、全体の整合が保たれるようなシステム（ＩＴシステムではなく体制の意味でのシステム）を構築する。

そのようなマネジメントシステムが構築されていることを、第三者が評価して認証する制度のひとつが ISMS である。

したがって、マネジメントシステムに関する認証を取得しているということは、ある時点における、対策レベルが一定の状態であることを認証するものでは必ずしもない。

そのため、例えば、認証を取得している組織について、将来の事故の発生がないことが保証されているものではないことに注意しなければならない。

5.6.2　リスクの許容レベルの安定性

残存リスクを許容する程度については、ISMS 認証取得範囲組織の対策責任者（プライバシーマークの取得範囲は事業者全体のみであるため、事業者全体の責任者のみ）が判断することになる。したがって、認証を取得しているということは、その責任者の考える許容リスクレベルと、組織内の実態が同程度になるようなマネジメントシステムが構築されているということである。極端に単純化して言えば、責任者についての有言実行がマネジメントされる体制になっているということが認証されている。そのため、志の高い責任者の下で、許容リスクが低く抑えられれば、対策レベルが高く保たれていることになるが、そうではない責任者の下では、許容リスクが比較的高くなり、低い対策レベルが許容される状態になる可能性がある。前者については、許容リスクが低く抑えられた場合の話しであり、事業者としてハイ・リスク・ハイ・リターンを取るという判断が事業側にあれば、必ずしも低く抑えられるとは限らない点にも着目する必要がある。マネジメントシステム認証においては、残存リスクが認識されているか否かの観点を重視するため、その残存リスクがあまりに一般常識からかけ離れていない限りは、残存リスクの妥当性については、責任者が判断したものによることになる。すなわち、高いリスクであっても、それが高いということを責任者が正しく認識して選択しているのであれば、高いリスクを選択していることがマネジメントシステムの適合性がないと判断されることはない。

この点は、ISO 9000 として知られる品質保証マネジメントシステムについても同じである 。しかし、たとえば製造物製品であれば、その製品における主要な安全性については、製品の種類ごとに品質基準が法的に又は業界により定められており、それに準拠することが要求されている。そのため、責任者が許容する残存リスクがそれらの水準よりも高く取られることは、コンプライアンス上の違反として適合性が認められないことにより、マネジメントシステムの適合性評価によって、対策レベルの最低水準がある程度保たれることになる。一方で、情報処理についてはその入力と出力は、業種業態や情報を取り扱う作業個別に態様がまったく異なるため、広範に一般化することができない。たとえば、クレジットカードの取り扱いについては、PCI DSS（Payment Card Industry Data Security Standard）で一定の基準を定めているが、これが可能なのは、クレジットカードに関連するデータが国際的に定型化されていること及び支払い決済の業務フローを前提とするデータ処理作業範囲であることの２点が特定されているからである。しかし、PCI DSS においても、クレジットカードの取り扱い場面に違いがあることから、具体的な対策レベルを一意のものにはできていない。

そのようにデータとそれを処理する作業が特定されない限り、リスクの許容レベルを一般化することは難しく、さらに許容レベルを一般化できても対策レベルを具体的に一般化するには処理

の態様を細分化する必要があり困難である。許容レベルを適切に選択し、それに見合った適切な対策方法を決定するには、責任者が適切に判断することに期待するしかない部分が多いのである。特にデータ種別の特定のない場合には、ベースライン手法と言われる、最低限のレベルを固定することすらままならないことも多い。

5.7 組織のマネジメントシステムと委託先の関係

5.7.1 業務委託関係と情報提供関係

業務委託においては、委託する業務を管理する場合には、委託元が委託先を管理することになる。しかし、業務委託における情報の管理については、必ずしも委託元から委託先になるとは限らない点について注意する必要がある。

業務委託をする場合に、委託元と委託先間でやりとりする情報のうち、機密保持などのように、相手方に特段の管理を求める必要のある情報がどちらからどちらに提供されるのかは、委託する業務内容によって異なる。一例として、委託先から機密情報を委託先に提供する業務が考えられるが、その提供方向に限られることではない。委託先の機密情報が委託元に提供されることもあり得る。すなわち、業務委託の委託元及び委託先の関係と、情報提供の提供元及び提供先の関係は一意ではなく、業務内容によって変わるものである。

このため、業務委託の契約において、情報の守秘義務について契約条項又は別添の機密保持契約等において言及する場合には、それが片務になるか双務になるか、片務の場合にどちらからどちらになるかは一意ではなく、委託する業務内容によって個々に決まる。

したがって、情報セキュリティのマネジメントシステムにおいて、外部委託における情報管理については、情報の提供先への管理をする必要がある。その意味では、委託先の管理という表現は本来正確なものではない。提供先への管理という着眼をすれば、提供を受けた場合の管理という点についても考える必要性が自明のものとなりやすい。それに対して、委託先の管理という語感からは、片務であるかのような先入観になりやすい点に注意すべきである。

5.7.2 リスクの許容レベルの一貫性

業務委託でやりとりする情報について、情報セキュリティ対策が必要な場合には、その対策の残存リスクの許容レベルは、情報の提供者 が決定する必要がある。

業務委託において、委託元が管理責任を持つ情報を委託先に提供する場合には、その管理対策におけるリスク許容レベルは、委託元が決定した上で、委託先に指示して一貫性を保つ必要がある。

なぜなら、そのように決定しなければ以下のとおり、一貫性は担保されない。

委託先における ISMS 構築及び ISMS 認証取得では、情報セキュリティ対策における許容リスクのレベルは委託先の責任者の判断によって決定されることになる。このとき、委託先が業務委託で受領する情報を、それ以外と区別している場合においては、その許容レベルは情報の提供者からの指示に従った対策を講じるように定めているはずであるが、その指示がなければ受領を拒否することに定めていない限り、それ以外と同程度のものとして対策をするよう定めていると考えるのが自然である。一方、業務委託で受領する情報を区別していない場合は、本来は、情報の分別が不十分と言えるが、結果的にそれ以外の情報に対する対策と同じ管理がなされることになる。

どちらにおいても、情報の提供元がリスクの許容レベルを指示しない場合には、当該情報に対するリスクの許容レベルは、委託先の判断によるところとなり、委託元のそれと同じレベルになることは担保されなくなる。当該情報を取り扱う業務の情報管理対策について、法的な又は業界による対策基準が定められていれば、そのコンプライアンスとしてベースラインが保証されることはあるが、先に述べたとおり、そのような基準が定められているデータや業務は極一部に限られているのが現状である。

5.8 現状の問題と適切な活用方法

5.8.1 散見される問題

これまで述べてきた事項を再認識すれば、委託元が委託先に、ISMS 認証の取得だけを条件とすることは、委託元における ISMS 構築としては不十分なものであることは自明であろう。ところが、世の中では、「委託元が委託先に、ISMS 認証の取得を求める」ということが散見される。

この問題を正しく認識できている場合には、次の一文の意味を正確に理解することができよう。

「委託元と委託先の両組織において、ISMS が構築され認証されていることは、両者間で機密情

報のやりとりをした際に、情報の提供元が期待する情報セキュリティがその提供先で実施されることの担保のための十分条件にはならない。」

十分条件ではないとしても必要条件として使えるのではないか？と思われるかもしれないが、必要条件として有効に役立てることができるのは、相当限られた状況だけであって、一般的に言えば要求条件というよりも、参考情報程度にしかならないことも考えられる。理由は以下のとおりである。

5.8.2 適切な指示

前節の一文における担保のために必要なことは、情報の提供元が提供先に情報セキュリティ対策の内容を具体的に指示した上で、それの実施義務を提供先が約束することである。提供先では、指示された対策について、同程度の対策になると思われる代替策の方が、実効性や費用対効果が高いと考えられるならば、提供元の了解を事前に得た上で代替策を認めてもらえる場合があるかもしれない。しかし、提供元が了解しないならば、指示された対策を講じなければならない。このとき、指示されたとおりの対策を実施するということについて、提供先のマネジメントシステムに基づくのかと言えば、疑問である。マネジメントシステムにこだわるのであれば、むしろ、提供元のマネジメントシステムの配下に提供先を入るべきと言える。提供先のマネジメントシステムにこだわる人は、相手先組織の者を直接管理するよりも、その者は所属組織の管理下にある方がよい。と主張するかもしれないが、それは論点のすり替えだ。組織が人を管理するモデルとしてそれは正しいが、それを ISMS 構築や認証で担保することとは別の話しだからである。それを承知の上で、指示されたことを守るという点だけについて、相手先組織のマネジメントシステムを活用するということであれば、有り得なくはない。

しかし、提供元が具体的に指示した実施策を実施するだけなのであるから、契約上の履行義務を実施するだけのことであると考えた上で、提供先に ISMS 認証取得を求めることの効用に注意すべきである。

ここで、情報の提供者が提供先に情報セキュリティ対策を具体的に指示するのは、定型サービスを利用する際には非現実的だという反論は正しいが、冒頭に示したとおり、本項では、定型サービスについて論じていない。

5.8.3 指示の適切な時制

適切な対策について具体的に指示することが必要であることを述べたが、その指示は、情報を提供する前に実施しなければならない。機密として取り扱って欲しい情報を提供して、その情報の取り扱いが開始されてしまってから、その対策を求めても、既に手遅れになってしまうような処理も想定されることから、当然のことである。この点については、委託元が委託先に ISMS 認証の取得を求めることの有効性の確認において、さらに現状の問題を顕在化させるのに役立つ。

指示された対策を提供先が実施するのに、マネジメントシステムを役立てるということは前節で有り得るとした。このとき、それが役立てられるとすると、提供先の組織における対策で、「他の組織から機密として取り扱うように預かった情報については、当該情報の提供者からの対策指示に従うこと。」と定められている必要がある。そして、これについてマネジメントシステムが正しく構築されているならば、「対策指示の内容が明確ではない場合には、それが明確になるまで、当該情報を受領してはならない。」という管理がされているべきであろう。そのようなマネジメントシステムが構築されていることにより、自組織の者が対策指示を忘れて情報を提供してしまうことが、相手方によって未然に防がれるという状態を期待できる。これは、両組織においてマネジメントシステムがあることが有効になる例である。

しかし、これが定められていない場合には、「提供元からの指示を守る」という対策がないわけであるから、その組織内では逆に、他の組織からの指示を受けることはマネジメントシステム上の問題である。マネジメントシステムが構築されているならば、自組織の対策と指示された対策が異なってしまうということが有り得る。このとき、どちらの対策に準じるかが作業者の判断によるのでは、本当のところ、その組織のマネジメントシステムは適当とは言えない。

したがって、情報の提供元が提供先に対策を指示するのは、情報の提供に先んじることは当然であるが、ISMS 認証の取得を求める場合には、上記のような提供者からの指示に従う旨の対策がなければならない。しかし、業務委託の契約後に、対策指示の内容が変動することは、ビジネス上容認されるものとはなりにくい。そのため、「提供者の指示に従うこと」といっても、暗黙には「提供者からの指示について組織が予め合意した内容に従うこと」として運用せざるを得ないは

ずである。この点についても理解した上で、相手方に ISMS 認証取得を求めることの効用を考える必要がある。

5.8.4 法制度検討時の留意事項

以上のことから、情報セキュリティについての法制度を検討する際に、マネジメントシステムの適合性評価制度の活用を考える場合には以下のことに留意する必要がある。

(1) その制度が拠り所とするような、情報管理対策の最低水準レベルを示したものがあるかどうか。又は、それを示すことを含めた検討とするかどうか。

マネジメントシステムは、対策レベルを一定に保証するものではない以上、対策についての最低水準レベルがコンプライアンスとして求められない限りにおいて、対策レベルの保証とは無縁である。最低水準を示すものがあるかどうかで、法制度が何を期待できるのかの前提は大きく変わる点に留意すべきである。あるいは、法制度で新たにそれを示すということにすればよいが、情報管理においては、相当に細分化した個別の場合分けをしない限り、一定のレベルを示すことはできないと考えるべきである。

(2) 外部委託の場面では、指示に従うということ以上のことについて何を期待するのか。また、未来の行為についての認証を求めることの効用をどのように位置づけるのか。

外部委託の場面で、マネジメントシステムの適合性評価制度を、他の組織に求めることは、指示した対策に従うことという以上のことはすぐには考えにくい。それだけであるならば、契約履行義務でしかない。その上で、何を期待するのかに留意すべきである。また、何かを期待したとしても、未来に起こる行為でしかない。そのことについて、事前に取得しておく認証制度をどのように役立てるのかは、具体的に考えるべきである。

(3) 外部委託の場面では、指示に不備があった場合の結果責任の分担をどのように考えるのか。

外部委託の場面では、マネジメントシステムに基づいて指示された対策を実施するのであれば、その指示内容よりも有用な代替策が考えられる場合でも、指示を改めて受けなおす必要がある。従って、いずれの場合にも指示に従うことが基本となる。想定外の問題が生じた場合の結果責任については、普通に考えれば、指示者の想定外であれば、実施者が責任を問われることにはならないかもしれない。実施者が責任を問われるのは、指示に違反した場合に限られるのかに留意すべきである。その場合には、それは契約履行義務とは何が異なるのかを考えるべきである。

第 3 編　実証研究編

1　情報セキュリティのガバナンスと逸脱行動に関する調査

以下は、2009 年度の要約版である。報告書本編は、別に添付する。この調査に先立って、2008 年度には、情報セキュリティと「エンゲージメント」「ソーシャル・キャピタル」に関する調査を実施した。その成果は、別添の富士通総研調査レポート第 345 号(2009 年 6 月)にて公表されている。

1.1　調査の概要

1.1.1　調査の目的

本調査は、研究開発プロジェクト「企業における情報セキュリティの実効性あるガバナンス制度のあり方」の一環として、情報の持ち出しを中心とした情報セキュリティ関連ルールからの逸脱に関する実態調査を行い、情報システムの利用者の観点から、情報セキュリティの実効性を高めるために必要なガバナンス構造およびマネジメントのあり方を明らかにすることを目的として実施した。

1.1.2　調査の方法と対象

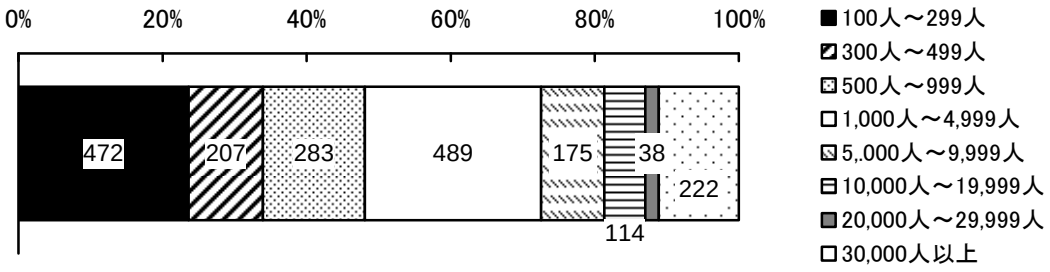
調査の方法および対象は、以下のとおりである。

- 方法＝インターネット調査会社（株式会社ネットマイル）のモニターを対象とするウェブ調査
- 対象＝インターネット調査会社のモニターのうち、従業員 100 人以上の会社の社員（派遣社員を含む）で、業務で個人情報または機密情報を扱っている人。
- 回収サンプル数：2,000
- 調査実施時期は 2009 年 9 月

1.1.3　回答者の主な属性

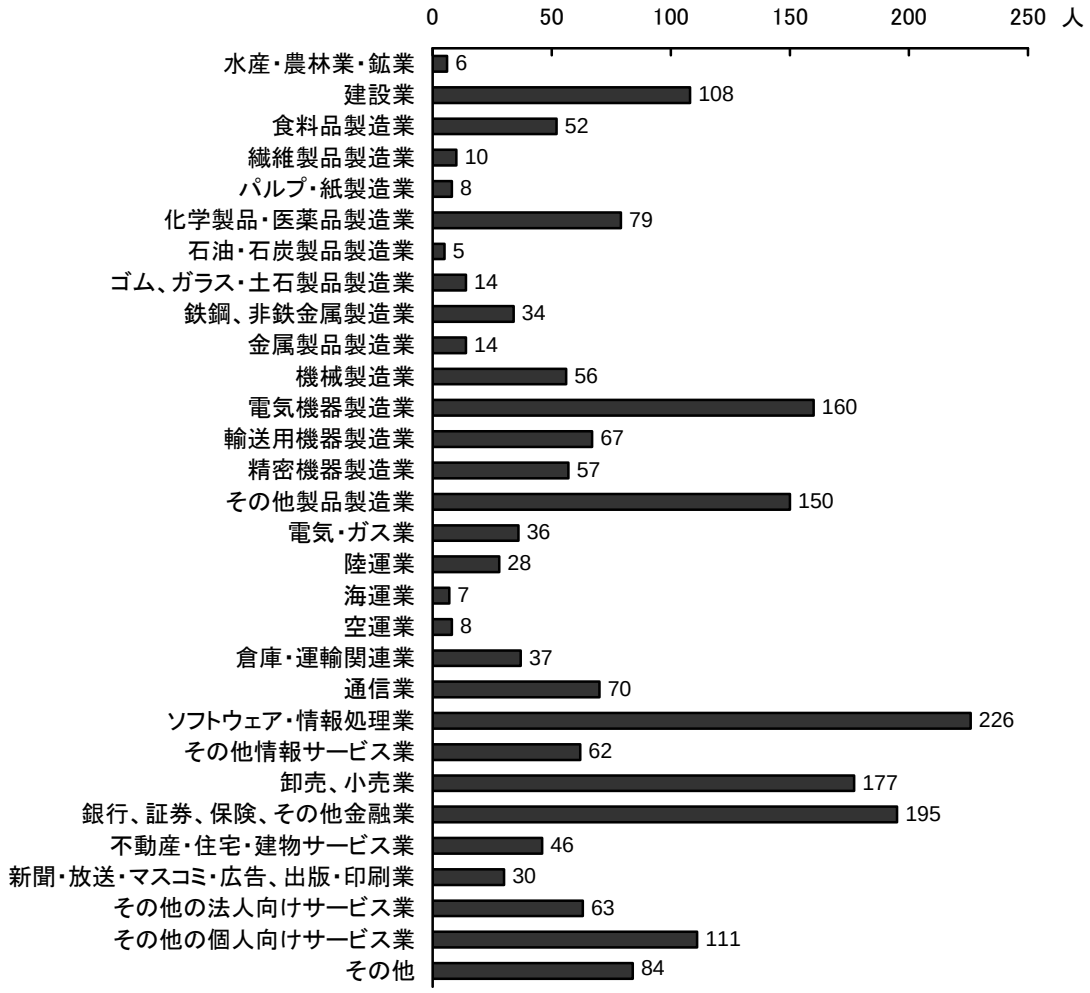
図表 1は、回答者が所属している企業の従業員数別の分布を示している。もっとも回答者が多いのは従業員 1,000 人以上 5,000 人未満の会社の社員である。

図表 1. 回答者の所属企業の従業員数別分布



図表 2は、調査に回答した 2000 名が所属する企業の業種別分布を示している。もっとも回答者が多い業種は「ソフトウェア・情報処理業」（226 人）で、二番目は「銀行、証券、保険、その他金融業」（195 人）である。「水産・農林業、鉱業」（6 人）、「パルプ・紙製造業」（8 人）、「石油・石炭製品製造業」（5 人）、「海運業」（7 人）、「空運業」（8 人）は、いずれも回答者が 10 名未満であった。

図表 2. 回答者の所属企業の業種別分布

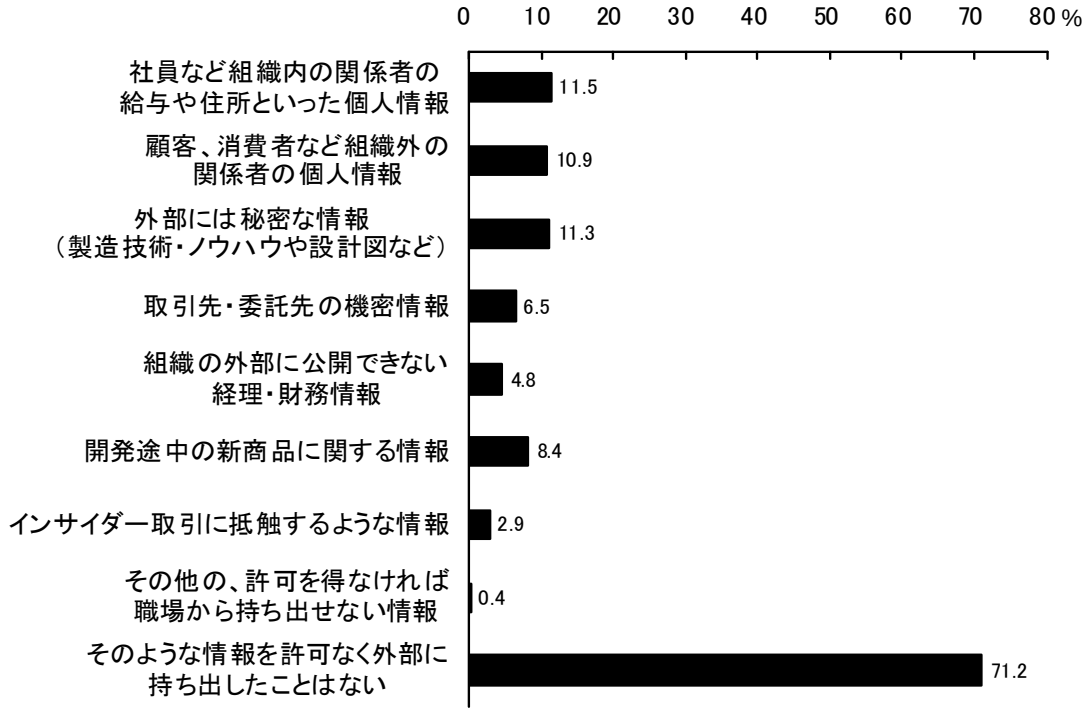


2　情報持ち出しおよび漏洩リスクのある行動に関するルールからの逸脱状況

2.1　情報持ち出しの状況

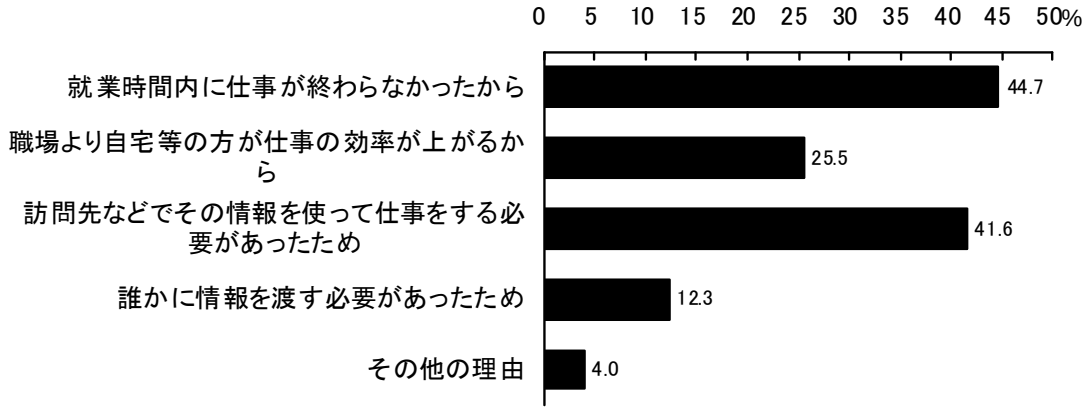
図表 3は、回答者自身が、最近５年間に、社内の機密情報や個人情報を許可なく社外に持ち出したことがあるかどうかを聞いた質問の回答である。機密情報や個人情報を許可なく社外に持ち出すことは、原則としてどのような会社でも禁止されていることであり、これはルールからの逸脱状況を示しているといえる。2000 人中 576 人（28.8%）の人が何らかの情報を許可なく持ち出したことがあると答えており、もっとも多いのは「社員など組織内の関係者の給与や住所といった個人情報」（11.5%）である。

図表 3. 許可のない情報持ち出しの状況



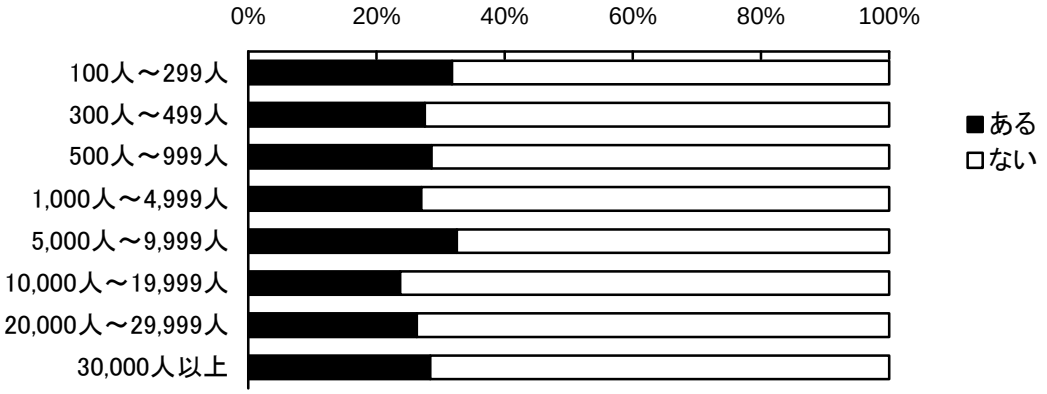
図表 4は、機密情報や個人情報を許可なく社外に持ち出したことがあると回答した人たち（576 人）に対して、その理由を聞いた質問の回答をまとめたものである。もっとも多いのは「就業時間内に仕事が終わらなかったから」（44.7%）であり、次いで「訪問先などでその情報を使って仕事をする必要があったため」（41.6%）という理由も多い。

図表 4. 機密情報・個人情報を社外に持ち出した理由

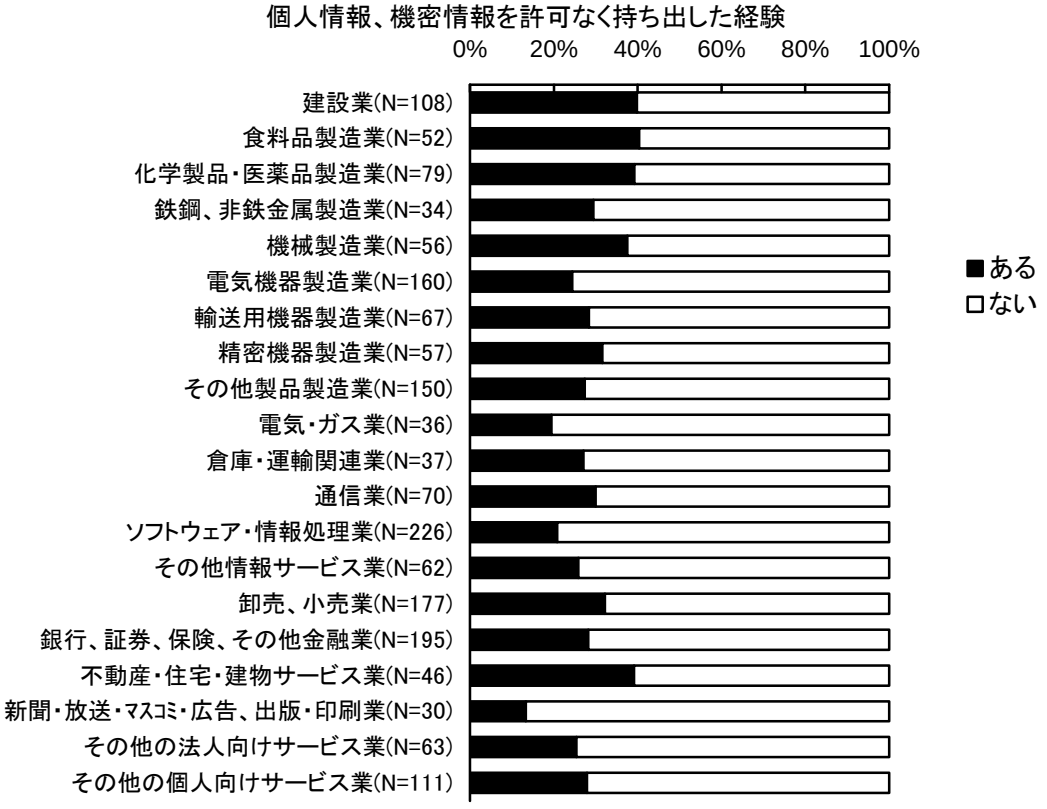


ルールを破って情報を持ち出したことのある人たちが所属する会社の属性を調べると、従業員数別には明確な特徴はないが、業種別には「ソフトウェア・情報処理業」や「銀行、証券、保険、その他金融業」では、そのような回答者の比率が他業種に比べて低い（図表 5、図表 6参照）。これらの業種の会社では、万が一漏洩が起きた場合の影響が大きく、社員は情報セキュリティに敏感であり、意図的なルールからの逸脱が他業種よりは比率としては少ないと言える。

図表 5. 従業員数別の情報持ち出し行為の有無



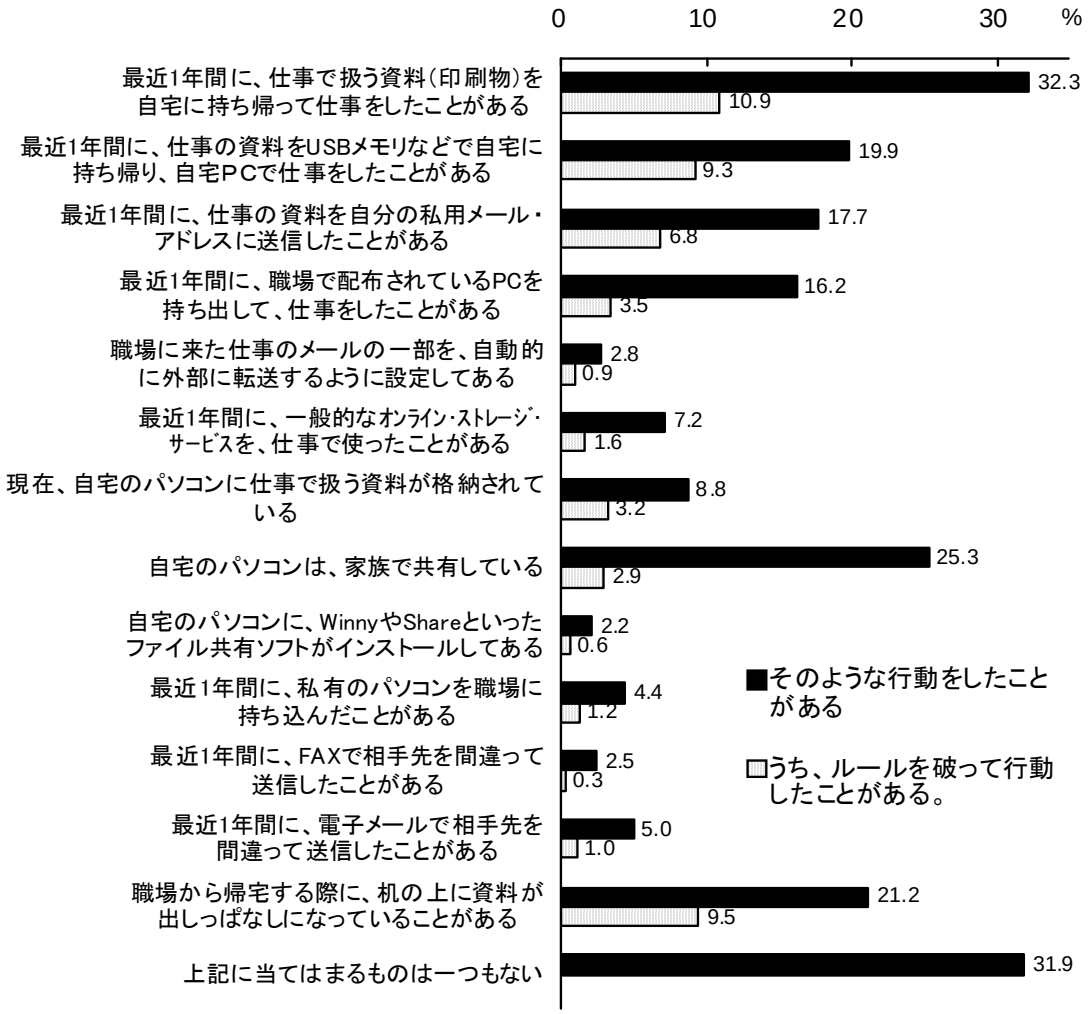
図表 6. 業種別の情報持ち出し行為の有無（回答者が 30 人以上の業種のみ）



2.2 漏洩リスク行動の状況

図表 7は、会社資料の自宅への持ち帰りから家庭ＰＣの家族での共有まで、リスクの大きさはさまざまであるが、少しでも情報漏洩につながる可能性のある行為について、回答者が経験しているかどうか、その行為が会社のルールから逸脱したものであるかどうか、ということを聞いた結果を示している。たとえば、「最近 1 年間に仕事で扱う資料（印刷物）を自宅に持ち帰って仕事をしたことがある」人は 2000 人中 646 人（32.3%）であり、そのうち 70 人（10.9%）が会社のルールを破っている（残り 89.1%はルールを守っているか、ルールの存在を知らないか、どちらか）。

図表 7. 情報漏洩につながるリスクのある行為の実施状況



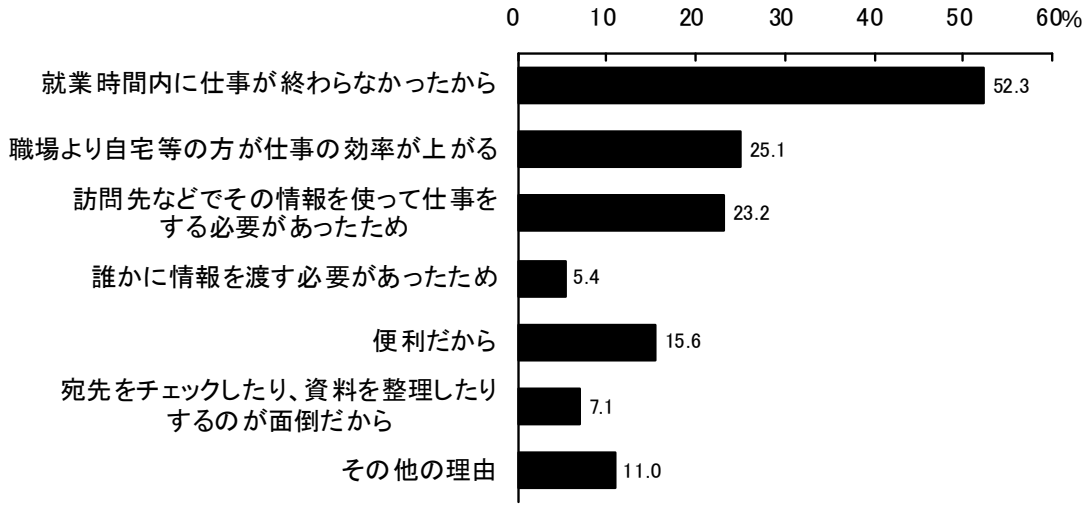
図表 8は、回答者がどの程度情報漏洩のリスクがある行為を行っているかということをまとめたものである。ここでは、図表 7 に示したような行為をまったく行っていない場合を「無リスク」、そのような行為を一つ以上行っているが、ルールを破っているわけではない場合を「低リスク」、ルールを意識的に破ってそのような行為を行っている場合を「高リスク」と分類し、それぞれの人数を集計した。「低リスク」と分類した回答者は、正確には、ルールの存在を知って守っていた場合と、そもそもルールの存在を知らなかった場合とが考えられ、リスクの程度という意味では両者は本来区別されるべきだが、今回の調査ではその区別は調べることができなかったため、ここでは同じものとして扱っている。

図表 8. 情報漏洩リスクの程度

		N	%
無リスク	情報漏洩につながるような行動を行ったことがない	638	31.9
低リスク	情報漏洩につながるような行動を行ったことがあるが、ルールを破っているわけではない。	880	44.0
高リスク	ルールを意識的に破って、情報漏洩につながるような行動を行ったことがある。	482	24.1

高リスク行動をとっている 482 名について、なぜルールを破って情報漏洩につながる恐れのある行動を取っているのかを聞いた回答を集計したのが図表 9である。もっとも多いのが「就業時間内に仕事が終わらなかったから」で、半数以上がこれを高リスク行動の理由としている。

図表 9. 高リスク行動をとった理由

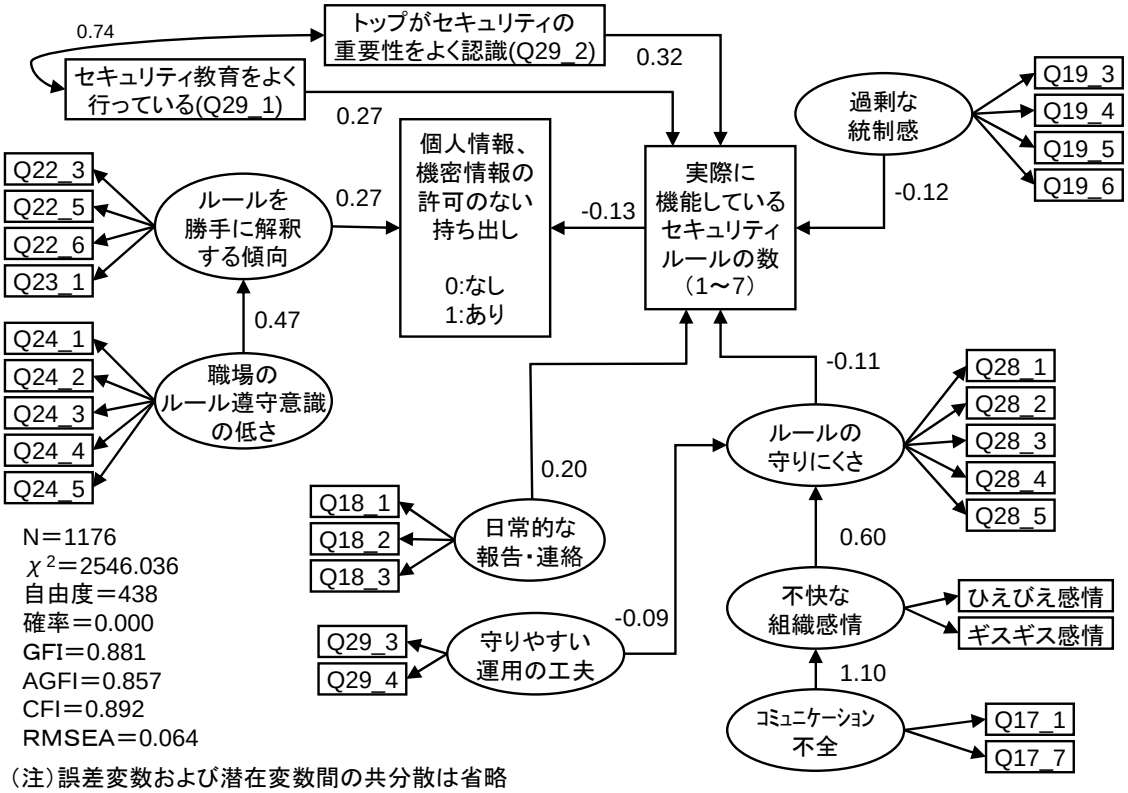


3　ルールからの逸脱の要因に関する検証

3.1　情報持ち出し行為に関するモデルの検証

図表 10は、情報持ち出し行為に関するモデルを検証した結果を示すパス図である。長方形はアンケート調査から直接観測される変数を表しており、楕円形はそれらの観測変数から合成される潜在的な因子を示している。また、変数間の矢印は因果関係を示しており、矢印に付いた数値は関係の強さを示すパス係数である（平均 0、標準偏差 1 に標準化された値）。

図表 10. 情報持ち出し行為に関するモデルの検証



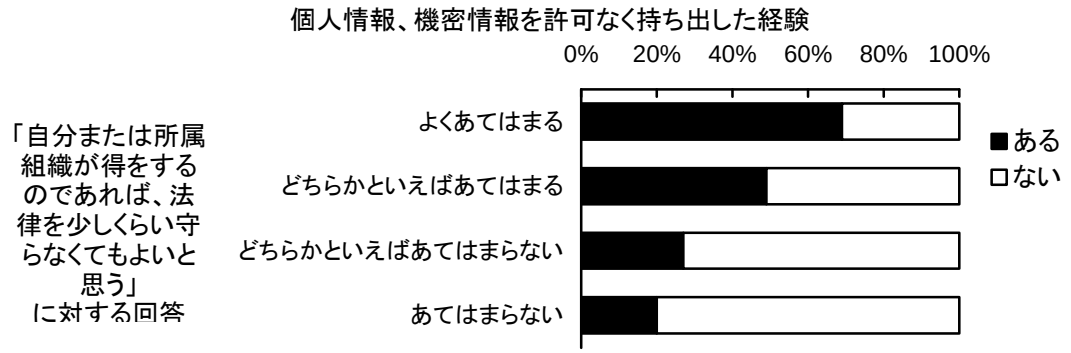
（注）誤差変数および潜在変数間の共分散は省略

このパス図からは、以下のようなことがわかる。

- 個人情報や機密情報の許可のない持ち出し（ルールからの逸脱）が促されるのは、ルールが存在しないか、存在していても機能していない場合、また、社員がルールを自分勝手に解釈してしまう傾向が強い場合である。社員がルールを勝手に解釈する傾向とは、具体的には以下のような項目で測定される。
  - ➢ 他人に迷惑がかからなければ、法律は守らなくてもよいと思う（Q22_3）
  - ➢ ルールというものは、自分なりに勝手に解釈して運用してもよいと思う（Q22_5）
  - ➢ 職場のルールは、法律ほど厳しいものではないから、破ってもよいと思う（Q22_6）
  - ➢ 自分または所属組織が得をするのであれば、法律を少しくらい守らなくてもよいと思う（Q23_1）

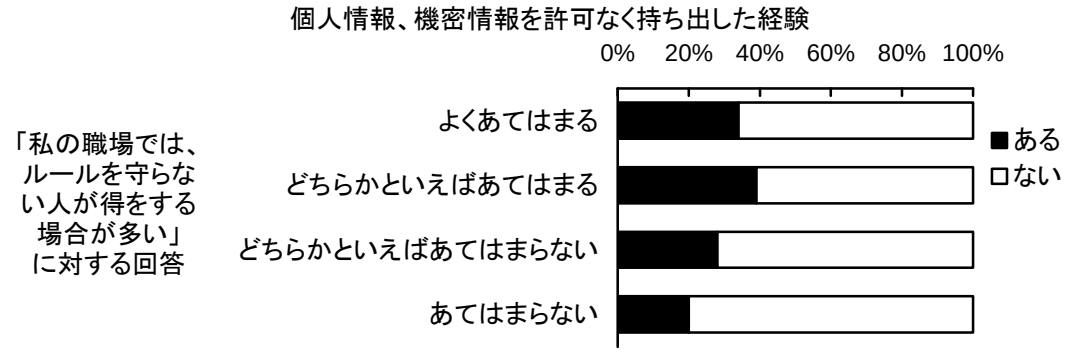
- たとえば、「自分または所属組織が得をするのであれば、法律を少しくらい守らなくてもよいと思う」という問いに「よくあてはまる」と答えた回答者は、「あてはまらない」という回答者よりも、明らかに情報持ち出しが多い（図表 11参照）。

図表 11. 回答者自身のルール意識と情報持ち出し行為



- 職場全体としてルールを守ることの認識が低い場合、個々の社員もルールを勝手に解釈するようになってしまい、その結果逸脱行動が多くなる。職場全体としてのルール認識が低いことは、具体的には以下のような項目で測定される。
  - 私の職場には、ルールを守らない人が多い（Q24_1）
  - 私の職場では、ルールを破る人がいても注意する人がいない（Q24_2）
  - 私の職場では、ルールを守らない人が得をする場合が多い（Q24_3）
  - 組織のためであれば、多少ルールを破ることも仕方がないという雰囲気がある（Q24_4）
  - 発覚さえしなければ、ルールを破ってもよいという雰囲気がある（Q24_5）
- たとえば「私の職場では、ルールを守らない人が得をする場合が多い」に対して「よくあてはまる」という回答者は、「あてはまらない」という回答者よりも、自分自身のルールを守るという認識が低く、結果的に情報持ち出し行為も多くなっている（図表 12参照）。

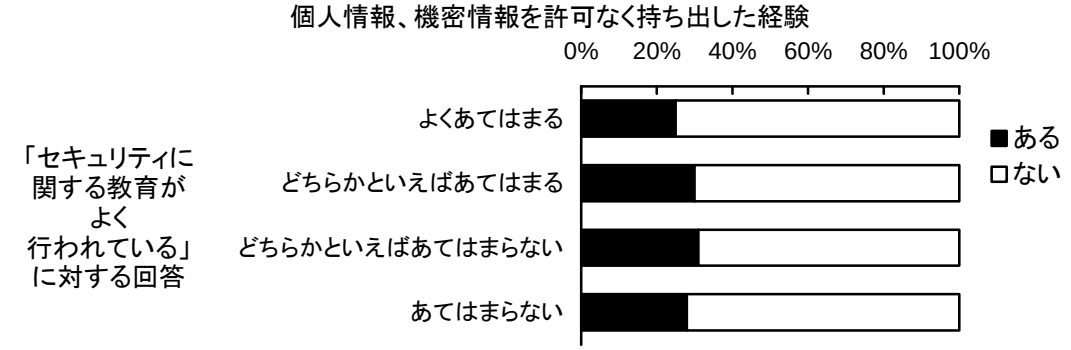
図表 12. 職場のルール意識と情報持ち出し行為



- 実際に機能しているルールの数が多いかどうかは、職場で日常的な連絡・報告が行われているか、過剰な統制が行われていないか、ルールが守りにくいと認識されていないか、という要因に左右される。また、職場における情報セキュリティ教育の実施状況および経営トップのセキュリティに対する認識にも大きな影響を受ける。
- 職場における情報セキュリティ教育の実施状況は、以下の質問に対する回答で測定される（「よくあてはまる」＝4、「あてはまらない」＝1）。
  - セキュリティに関する教育がよく行われている（Q29_1）

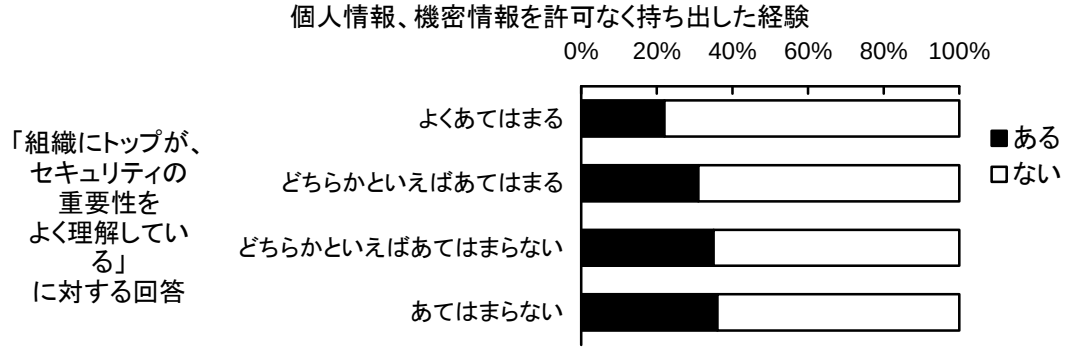
- 「セキュリティに関する教育がよく行われている」に対する回答が「よくあてはまる」の場合は、「あてはまらない」に比べて機能しているルールの数が多く、結果として、わずかではあるが情報持ち出しも少なくなっている（図表 13参照）。

図表 13. セキュリティ教育の実施状況と情報持ち出し行為



- 経営トップのセキュリティに対する認識は、以下の質問に対する回答で測定される。
  - 組織のトップが、セキュリティの重要性をよく理解している（Q29_2）
- 「組織のトップが、セキュリティの重要性をよく理解している」に対する回答が「よくあてはまる」の場合は、「あてはまらない」に比べて機能しているルールの数が多く、結果として情報持ち出しも少なくなっている（図表 14参照）。

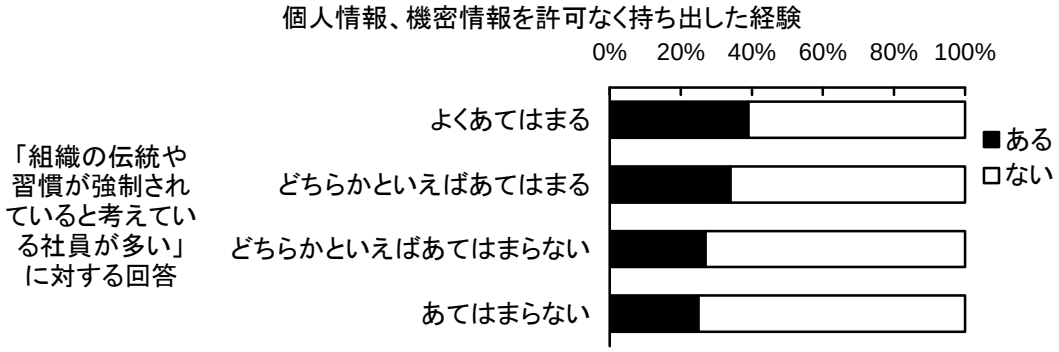
図表 14. トップの認識と情報持ち出し行為



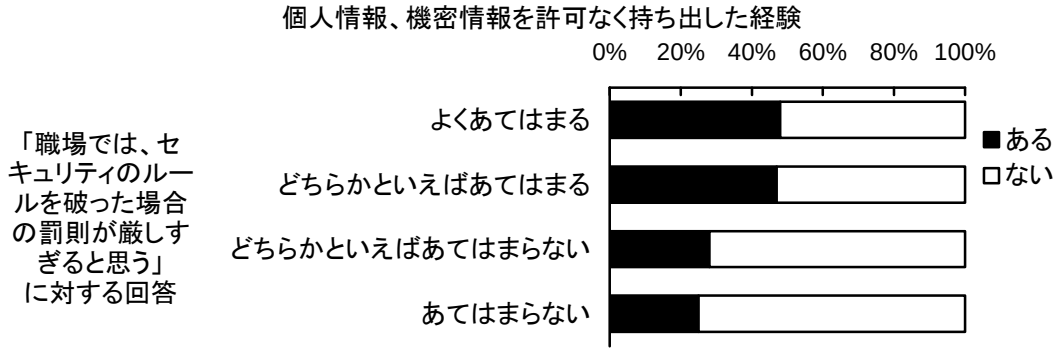
- 職場で日常的な連絡・報告が行われているかどうかは、以下のような項目で測定され、これらにあてはまる場合、ルールが機能し、逸脱行為も少なくなる。
  - 日常的に連絡・報告は必ず上司に実施することになっている（Q18_1）
  - 仕事で何かトラブルが発生したら、直ちに上司に連絡・報告することになっている（Q18_2）
  - 仕事については、全て上司に決裁を実施している（Q18_3）
- セキュリティに関する統制が厳しすぎる場合は、ルールは機能しなくなり、逸脱行動も多くなるという逆効果が発生する。統制が厳しすぎるとは、具体的には以下のような項目にあてはまる場合である。
  - 職場では、上司は、部下を非難はするものの、めったに信用しない（Q19_3）
  - 職場では、言われたことをすぐにやらないと、批判されるような雰囲気がある（Q19_4）
  - 組織の伝統や習慣が強制されていると考えている社員・職員が多い（Q19_5）
  - 組織が個人の存在を無視する傾向がある（Q19_6）

- たとえば「組織の伝統や習慣が強制されていると考えている社員が多い」に対して「よくあてはまる」という回答者は、「あてはまらない」よりも逸脱が多くなっており、統制が厳しすぎると逆効果になる（図表 15参照）。また、罰則が厳しすぎてもルールからの逸脱は抑止されないこともわかった（図表 16参照）。

図表 15. 職場の統制環境と情報持ち出し行為



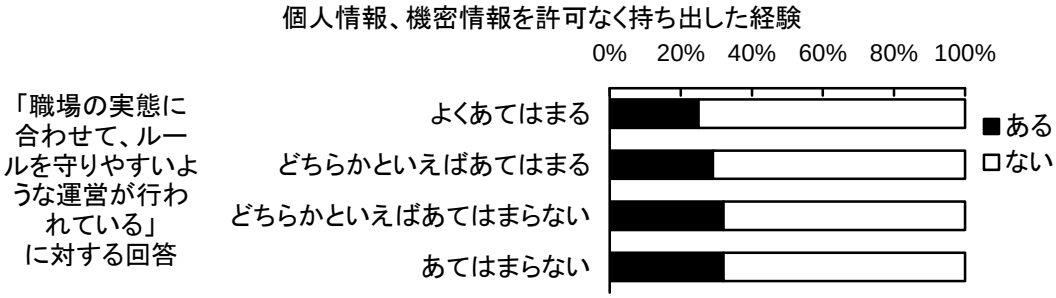
図表 16. セキュリティに関する罰則の厳しさと情報持ち出し行為



- ルールが存在したとしても、守りにくいと社員が考えている場合は、ルールも機能しなくなり、逸脱行動が多くなる。以下のような項目にあてはまる場合が多いと、ルールを守りにくいという意識が強くなる。
  - 職場の情報セキュリティに関するルールは、実際には守ることができないものが少なくない（Q28_1）
  - 職場のセキュリティに関するルールを定めた規程は、文章が多く、読む気にならない（Q28_2）
  - 情報セキュリティ対策のせいで、生産性が低下するなど、自分の仕事に支障が出ている（Q28_3）
  - 職場のセキュリティに関するルールは、運用が厳しすぎると思う（Q28_4）
  - 職場のセキュリティに関するルールを定めた規程は、読んだとしても内容がわからないものが多い（Q28_5）
- ルールを守りやすいような工夫が行われていれば、守りにくいという意識は減り、逸脱行為も抑制される。守りやすい工夫とは、具体的には以下のような項目である。
  - ルールを設定する際に、利用部門の意見を十分に聞いている（Q29_3）
  - 職場の実態に合わせて、ルールを守りやすいような運営が行われている（Q29_4）

- たとえば「職場の実態に合わせて、ルールを守りやすいような運営が行われている」に対して「あてはまる」という回答が多い場合、ルールを守りにくいという意識が弱くなり、結果としてルールからの逸脱も抑制される（図表 17参照）。つまり、職場の実態を無視してルールを運用したとしても逸脱行為は減らず、経営トップのコミットメントや職場の実態に合わせた運用、セキュリティ担当者と利用者の間の相互理解といったルール運用のあり方が逸脱抑止に効果的であることがわかる。

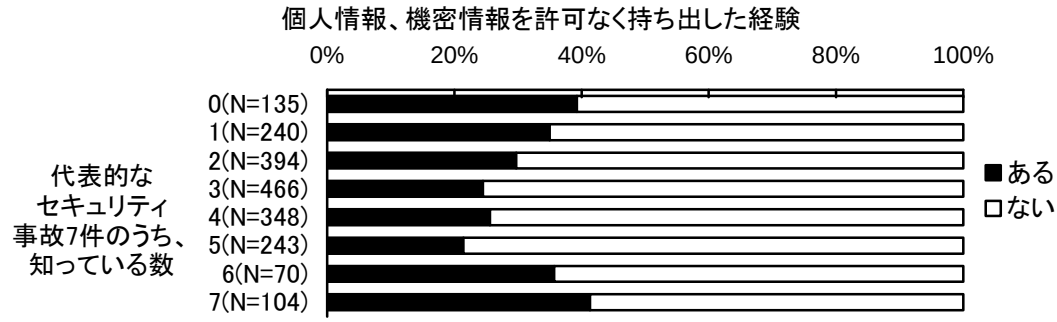
図表 17. ルールの運用方法と情報持ち出し行為



- 職場に「ギスギス感情」や「冷え冷え感情」といった不快な感情が強い場合、たとえ同じルールであったとしても、ルールを守りにくいという意識が強くなる。
- 職場のコミュニケーションが不全である場合、不快な組織感情が強くなる。
- コミュニケーションが不全であるとは、具体的には以下のような項目にあてはまる場合である。
  - 職場のコミュニケーションは、電子メールなど口頭以外のものが多い（Q17_1）
  - 一人ひとりの仕事が専門化されており、職場がタコツボ化している（Q17_7）

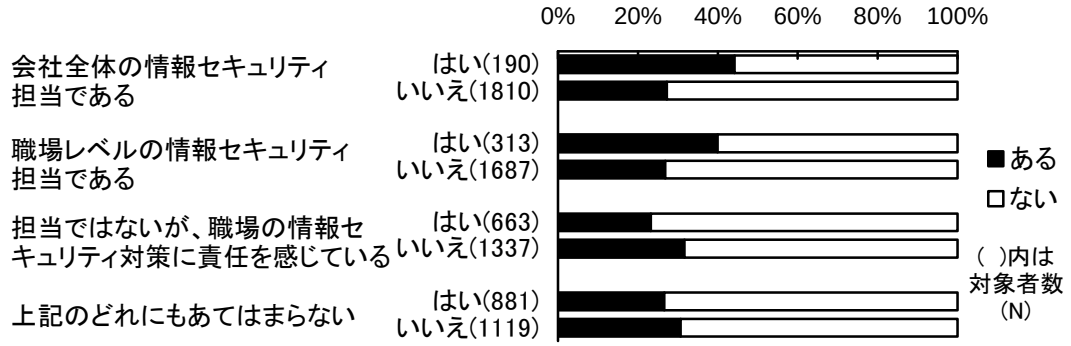
また、回答結果のクロス集計からは、回答者が個人的に情報セキュリティに関する知識を多く持っていたとしても、逸脱行動は抑止されていないこともわかった。むしろ逆に、情報セキュリティに詳しい回答者は、中程度の知識を持っている人たちよりも逸脱行動が多い傾向にあった（図表 18参照）。

図表 18. セキュリティ事件知識別の情報持ち出し行為の有無



さらに、今回のアンケート調査では、情報セキュリティ担当者自身の逸脱行動は、一般の非担当者よりも比率が高くなっていた（図表 19参照）。これらのことがらは、情報セキュリティに関する知識が増えれば増えるほど、「ルールから逸脱したとしても、自分だけは大丈夫」という意識が働くからだと解釈することもできるだろう。

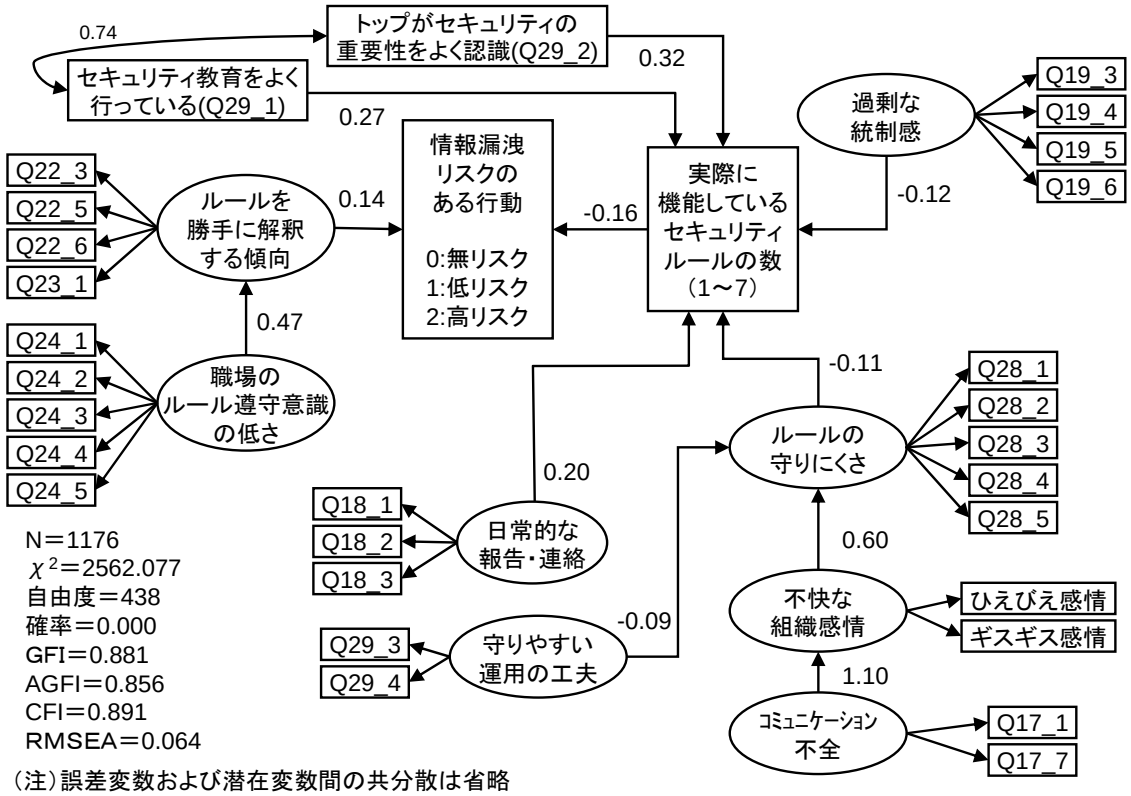
図表 19. セキュリティへの関与別の情報持ち出し行為の有無



3.2 漏洩リスク行動に関するモデルの検証

図表 20は、図表 10と同じモデルを漏洩リスク行動にあてはめた結果である。このモデルでは、回答者が情報漏洩につながるおそれのある行動をどの程度取っているかという変数を最終的な被説明変数にしている。その他は図表 10の情報持ち出しの場合と同じだが、この場合もモデル全体の適合度は高く、同じモデルがあてはまることを示している。

図表 20. 漏洩リスク行動に関するモデルの検証



（注）誤差変数および潜在変数間の共分散は省略

4　ガバナンス実効化のための提言

機密情報や個人情報の許可を得ない社外への持ち出し行為や、情報漏洩リスクの高い行動を抑制するためには、まずは、ルール自体を整備することが必要である。今回の調査からは、情報セキュリティポリシーのない会社ではポリシーが機能している会社よりも情報持ち出しが多くなっていることも明らかになっており、全体的なルールそのものの重要性を確認することができた。ＰＣの社外持ち出し制限といった具体的なルールの存在も、やはり逸脱行動の抑止に役立っている。

しかし、ルールが存在したとしても、十分に機能していなければ、情報持ち出しやリスクの高い行為は発生する。職場の実態を無視してルールを形式的に過度に厳格に運用すると、ルールは機能せず、逸脱行動も抑止できず、むしろ、厳しすぎる監視や罰則の存在は逆効果であることもわかった。

セキュリティ教育の実施など職場全体のセキュリティに対する意識を高めることは、逸脱行為を減らすために効果的だが、個人レベルで見れば、セキュリティに対する知識が高いほど逸脱行為が少ないかといえば、そうではない。知識が高い社員は、むしろ逆に逸脱行為が多い傾向にある。

逸脱を抑止するためには、ルールの制定やセキュリティ教育の実施といった対策のほかに、ルールを実効的に機能させることが必要であり、そのためには職場の実態に合わせた守りやすい運用が重要になる。具体的には、セキュリティ担当者が一方的に利用者にルールを押し付けるのではなく、担当者と利用者間の十分な話し合いによる相互理解、ルールの運用に関する利用者からの提言などが効果的である。

逸脱行動を少なくするためには、「ルールだから守る」という形式的な遵守を利用者に求めるよりも、トップ主導でそもそもなぜセキュリティ対策が必要なのかということを組織に浸透させることから、職場レベルで提案制度などによって守りやすい運用を行うことまで、ルール制定後のトップからボトムを巻き込んだ運用のあり方が重要である。情報セキュリティ教育も、社員のセキュリティに関する知識を形式的に高めることだけを目的にするのではなく、利用者が職場全体でセキュリティのあり方を自らの問題として考え、自ら進んでルールを守るという認識を醸成するためのきっかけとして考える方が実効性を高めることができるだろう。

2　ネットワークの情報流通と企業ガバナンスに関する調査

1 はじめに

わが国の企業では、特に従業員数の多い大企業において、個人情報保護等のために情報セキュリティ対策に積極的に取り組んでいる。しかし、情報セキュリティ対策は、ともすれば画一的なガイドラインの遵守を強制的に職場に押し付けるものが多く、組織における一つひとつの職場の実態を考慮していないものも少なくない。本報告書は、そのような現状に疑問を投げかける調査と検討を行った。

1.1　ネットワークの情報流通と企業ガバナンス

どのような企業や組織においても、ネットワーク（インターネット）は今や情報流通の要であり、厳密なセキュリティポリシーが適用された企業であっても、インターネットを介した情報流通は行っている。

最も典型的な例は電子メールであり、たとえ、高価で高機能なセキュリティツールを利用していても、その管理下でなにかしらのメール交換は行われている。同様に、企業活動において、厳しいアクセス制限を行ったとしても、Webを利用していない企業はない。

つまり、企業活動に伴って必ずネットワークを介した情報交換が発生する。この点に着目し、企業ネットワークに流れるトラフィックを観測することで、ネットワークに流通する情報と企業活動との関連性を調べ、画一的で厳しいセキュリティガイドラインの遵守が企業ガバナンスにおいて適切かどうかを検討する。

1.2 画一的で厳しいセキュリティポリシーの弊害

企業における情報セキュリティ対策は、ともすれば画一的なガイドラインの遵守を強制的に職場に押し付けるものが多く、組織における一つひとつの職場の実態を考慮していないものも少なくない。その前提のもとで浜屋が、情報セキュリティ対策の望ましいガバナンス構造を分析している[19]。分析において、セキュリティ対策と企業内の現場において、以下のような関係が成り立っていることが示されている。

- 情報セキュリティ対策は、効果があると認識されているが、一方で否定的な意識も生んでいる。
- 否定的な組織感情が強い職場では、情報セキュリティ対策に対する否定的な意識も強くなる。
- ソーシャル・キャピタルが不足している職場では、否定的な組織感情が強くなる。
- コミュニケーションが不足している職場では、ソーシャル・キャピタルの充実度も低い。
- ブログや SNS[20] といったEnterprise 2.0[21] 的なコミュニケーションツールの利用は、ソーシャル・キャピタルの充実に貢献している。
- セキュリティ担当者が利用者の視点に立っていると考えられているほど、セキュリティ対策の効果も強く認識されている。

このような分析結果の理由として、実際の企業におけるセキュリティ対策は非常に厳しいセキュリティポリシーの運用に基づき行われていることが起因していると考えられる。これは企業におけるコンプライアンスおよびガバナンス意識の強さから、それぞれの企業にふさわしいセキュリティポリシーの制定を行わず、教科書的かつ企業の立場からリスクが最も低くなる画一的な内容としているためであると考えられる。これは企業規模が大きくなればなるほどその傾向にある。

その結果、上述のソーシャル・キャピタル充実とは逆行するものとなっている。これは、ある意味、それぞれの企業独自のガバナンスという観点ではふさわしくない実態であるといえる。企業の立場からリスクが最も低くなるという消極的な姿勢が、むしろ企業内活動の停滞を招くという結果に他ならない。

---

[19]浜屋 敏「情報セキュリティ対策の望ましいガバナンス構造」経営情報学会 2009 年秋季全国研究発表大会

[20] これらの Web2.0 の代表的なサービスはソーシャルメディアと呼ばれ、ユーザが情報を発信し、形成していくメディアのことをさす。CGM（コンシューマー・ジェネレーテッド・メディア）とほぼ同義であり、ソーシャルメディアにはブログや SNS、インターネット上でお気に入りを共有する「ソーシャルブックマーク」、ソーシャルニュースサイト、オンライン百科事典、クチコミサイト、FAQ サイト、ビデオ投稿共有サイト、掲示板などがある。

[21] ハーバード・ビジネス・スクールのアンドリュー・マカフィー教授が提唱している概念で、Web 2.0 の世界で一般的になっているブログ、SNS などのいわゆるソーシャル・ソフトウェアを企業内で活用することをさす。

1.3 企業における禁止事項の一例

企業内におけるコミュニケーションツール（メッセージングツール）の利用制限についてSkypeを例に調査を行った。その結果は以下のようにまとめられる。

- 日本の大手企業とその関連会社では、そのほとんどがSkypeインストールおよび使用禁止にしている。
- 企業規模が小さくなれば禁止にしていない傾向がある。
- 中小企業でも、取引先の大手企業が関係者に対して使用禁止にしている場合がある。
- 外資系企業では、Skypeを禁止にしているところは少ない。しかしながら、それは厳密なセキュリティポリシーに基づいている。

Skypeなどのようなコミュニケーションツールは、インターネットを通じて従来のコミュニケーションにおける制約（時間、距離、コスト）の問題を解決できるツールである。これらを悪と定義し排除することは、画一的に厳しいセキュリティポリシーの結果である。

その中で、厳密なセキュリティポリシーに基づき、Skypeを禁止にしているところは少ないという外資系企業は、それぞれの企業実体に応じた対応がなされている結果といえる。

2 ネットワークトラフィックによる企業活動の分析

先に述べたように、どのような企業や組織においても、ネットワーク（インターネット）は今や情報流通の要であり、厳密なセキュリティポリシーが適用された企業であっても、インターネットを介した情報流通は行っている。そのような背景において、企業における個人の活動実態を測る手段として、ネットワークトラフィック分析は有効と考える。

2.1 トラフィック解析の有効性

企業活動に伴って必ずネットワークを介した情報交換が発生する。例えば、取引先とのメールのやりとりひとつをとってもそうである。そしてなにより、企業活動に伴ってWebアクセスは必ず発生する。業務に関連する情報収集、ニュース等の社会情勢の参照など例をあげればきりがないが、企業内の個々人の活動の結果として必ずネットワークトラフィックが発生している。

トラフィック分析の長所は個々人の行動を分析する必要がないことである。ネットワークトラフィックは必ず企業外部との接続点に集約されるため、そのような要所における観測で分析ができることが最大のメリットである。

2.2 トラフィック解析の方法

インターネットを利用する際には、ゲートウェイと呼ばれる社内と社外をつなぐポイントが存在する。ゲートウェイでは、企業内外とやりとりされるトラフィックがすべて集約されており、図1のようにここを観測することによってトラフィック解析を行う。

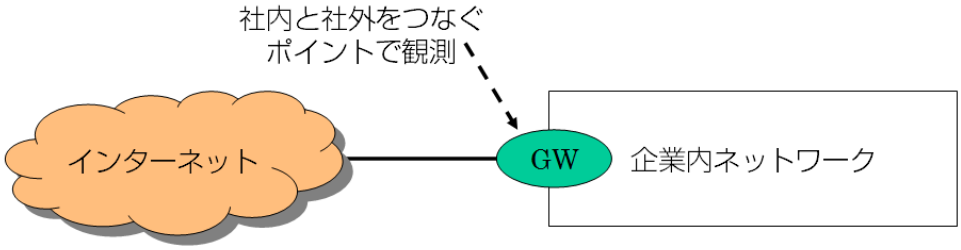


図1: トラフィック観測ポイント

このような方法をとることで、例えばWebアクセスのような典型的なプロトコル（情報交換手段）の通信相手先を観測するだけでよく、複雑なしくみを用いることなく観測が可能である。また、通信内容自体（必要なのは通信の付随情報）を見る必要がなく、SSLアクセスのように内容が暗号化された通信も観測可能であること、手法がシンプルなのでさまざまな企業で調査が可能である。

2.3 属性分類による企業内活動の判定

本調査では、トラフィック観測の結果を属性に分類することで、企業内活動の判定を行った。属性とはトラフィックを発生させる個々のアクセスが、どのような情報であるかの分類である。判別を行った属性は以下のとおりである。

search:	検索エンジン
work:	業務関連のサイト（ドメイン）
news:	ニュースサイト
blog:	mixi、hatena等のブログ、SNS
video:	動画投稿サイト
shop:	ショッピング関連サイト
map:	地図サイト
mail:	Webメール関連
ad:	広告関連サイト（ユーザが明示的にしてアクセスするものではなく、バナー広告のように付随してアクセスが発生する）
app:	アプリケーション（ソフトウェア）関連サイト（自動アクセス含む）
analysis:	認証サーバやアクセス解析のサイト
ignore:	上記属性対象外、および属性判別不能なアクセス

このように分類することで、企業内の活動が業務範囲かおおむね判別可能である。例えば、blogやvide、shopといった属性は通常、業務範囲外である。検索エンジンのアクセスやニュースサイトについては、業務範囲内外どちらも含む可能性があるが、業務範囲外のアクセスも伴うことになるので判別可能である。またworkとは、実際に取引のある企業のドメインとのやりとりをこれに分類する。その他、ユーザが明示的にアクセスしなくても発生するもの、どれにも該当しないものも分類した。

なお、属性の判別については半自動で行った。これは、よく知られたサイトについてはデータベース化することで自動判別し、それ以外においては手動で振り分けを行っている。そのため完全な属性判別ができないアクセスはignoreに分類される。

2.4 アクセス数の計測方法について

トラフィック解析の処理を行う際、対象はWebトラフィックに限定し、アクセス数をベースに行う。アクセス数についてはシンプルにアクセス数（リクエスト数）ベースでカウントを行う。ただし、HTTPプロトコル[22]によるWebアクセスでは、ユーザのアクセス（リクエスト）に対して、複数の応答が発生する（ページによりその数も量も異なる）。そのため、純粋にHTTPを観測するのではなく、ユーザのアクションによるリクエストと考えられるアクセスを抽出する。そうして、ここで示すような各アドレス別のアクセスリストを時間帯別に作成してから属性分類を行う。

```
アドレス : アクセス数                    →捕捉説明
XXX.co.jp : 4,302                    →業務に関連する取引先とのやりとり
mail.google.com : 3,880
static.cache.l.google.com : 2,415
      →Google Chrome を使用すると、数秒おきにアクセスされる
www.google.co.jp : 2,216
bizad.nikkeibp.co.jp : 1,305         →日経BP社の総合ポータルサイト
b.hatena.ne.jp : 1,296               →はてなブックマーク
www.google.com : 1,199
YYY.co.jp : 1,080                    →業務に関連する取引先とのやりとり
ads.mixi.jp : 991                    →mixiの広告
toolbarqueries.google.co.jp : 964
      →Googole ツールバーを使用するとページランク取得のためにアクセスされる
ai.yimg.jp : 963 :                   →Yahoo 広告の画像関係
googleads.g.doubleclick.net : 952 →Googleの広告
www.yahoo.co.jp : 819
```

[22] Hypertext Transfer Protocol は Web ブラウザと Web サーバ間で HTML などの送受信に用いられる通信プロトコルであり、RFC2616 で規定されている。

r1.ace.advertising.com : 683
money.www.infoseek.co.jp : 668　→金融関係のポータルサイト

3 ネットワークトラフィックによる企業活動の分析結果

本調査においては、トラフィック解析を行うために観測ツールの作成を行った。作成ツールは観測ポイントにおいてWebトラフィックを記録し、記録したデータに対して通信相手のアドレスリスト（3.3に記述）から、通信の属性を判別（判別そのものは、簡易的な属性判別処理ロジックと人手での調整で対応）し、通信の属性から企業内の個々人の活動を判定した。また、直接観測できない場合には、本ツールにてファイヤウォールのログ（ログの出力設定と記録方法の設定は必要）を解析することで同様の調査が可能である。

3.1 調査対象

厳密なセキュリティポリシーを適用した企業でこのような分析を行っても、行動が制限されてしまっているため有意な結果は得られない。そこで、行動の制限が少ない企業において、どのような結果が出るかという観点で調査を行った。

実際、中小企業などでは、厳密なセキュリティポリシーを適用していない例が少なからず存在する（中小企業においても、IT 技術に明るくない企業であればコストをかけて画一的なセキュリティポリシーを適用しようと努力をしている可能性はある)。そこで今回、特にアクセス制限が行われていない小規模企業 I（10 人規模）と、厳しいセキュリティポリシーを適用していない中規模企業 N（100 人規模）を対象とした。

3.2 アクセス総数と全体の動向

分析は営業日（平日）を対象とし、各属性のアクセスの総数を時間帯別にグラフ化した。グラフ 1 においては企業 I にて、各属性のアクセスおよび、属性分類できないアクセス ignore、アクセスの総数（グラフでは sum）を示した。グラフ 2 は同様の計測を企業 N で行った結果である。

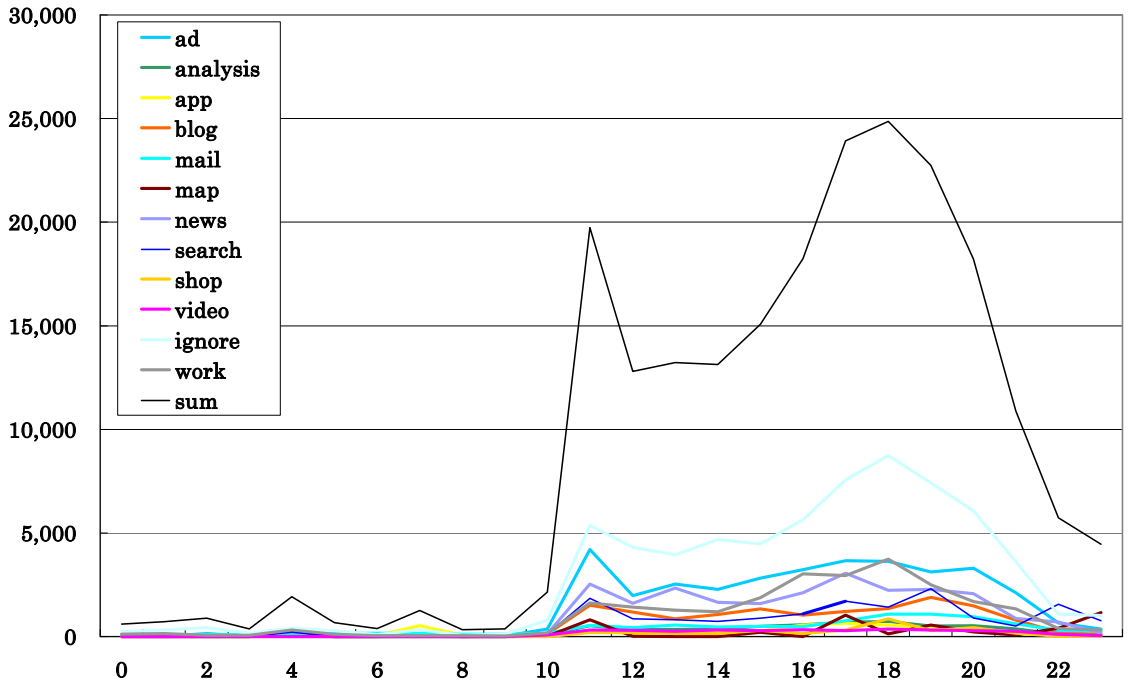
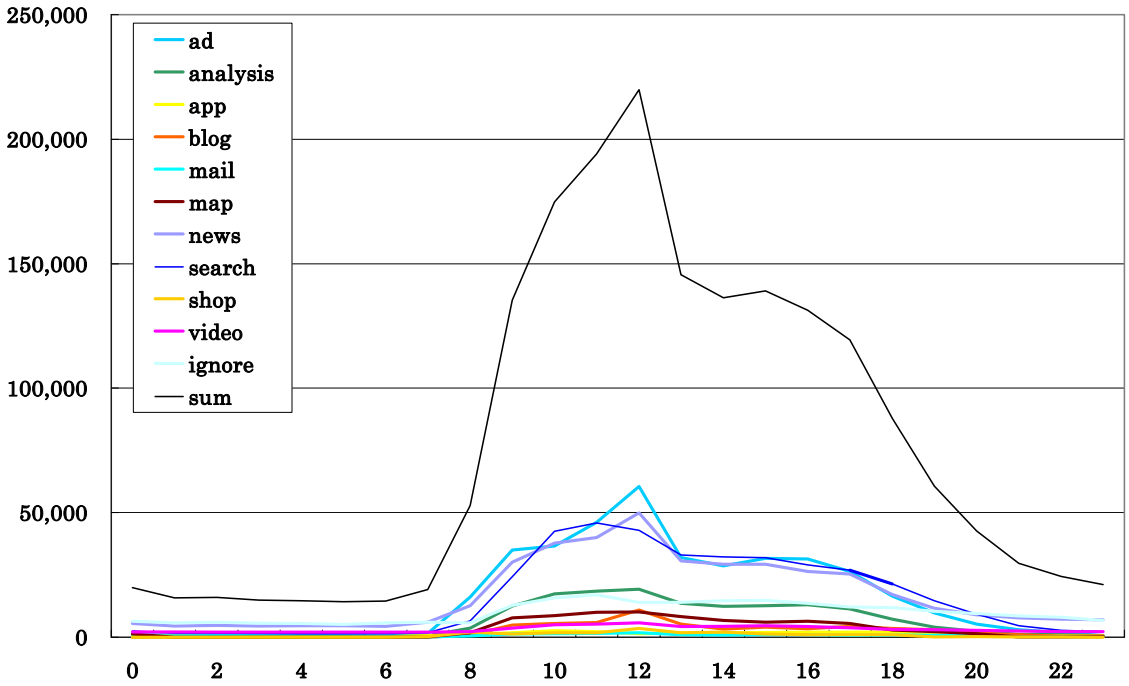


図 2: アクセス総数と全体の動向（小規模企業 I）



グラフ 2: アクセス総数と全体の動向（中規模企業 N）

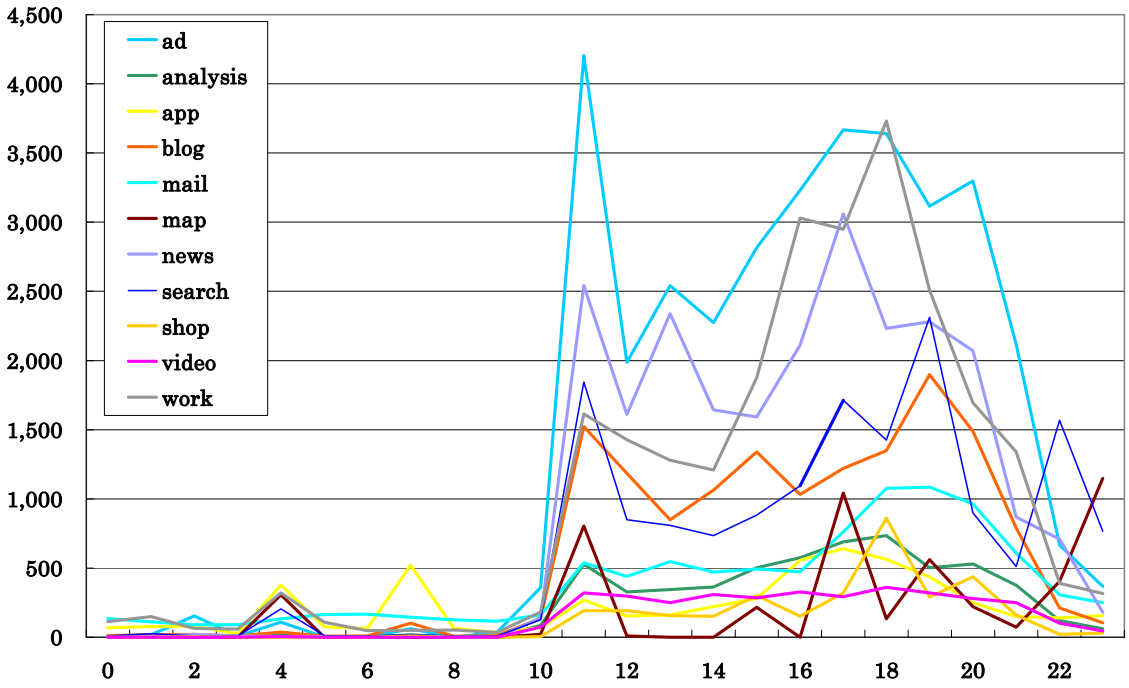
まずこれらのグラフより社員数のオーダが 1 桁違う I 社と N 社の規模がそのまま Web アクセス量に比例していることがわかる。アクセス総数のピークをみると、だたいその数が 10 倍程度の開きとなっている。なお、N 社については業務上の情報管理により work 属性のグラフは示していない。

また、企業の活動時間帯についても知ることができる。I 社はアクセスの立ち上がりが 10 時、N 社は 9 時となっている。ピークを迎える時間帯も 12 時前でどちらも同じである。社は規模の小さい開発会社の構成員の外出が少ないことが、ネットワークアクセスのピークが 18 時に向かって立ち上がっていることからも分かる。逆に N 社においては、午後は午前のピークより少なく、アクセスも分散している。

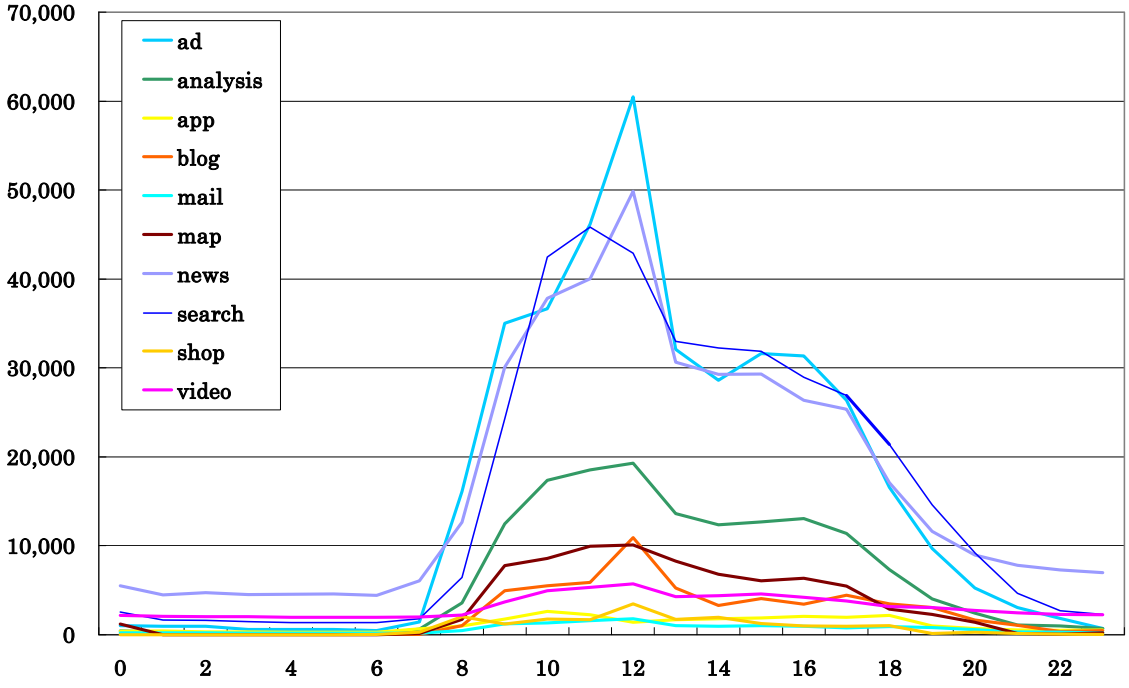
3.3 各属性別のアクセス動向

3.2 のグラフ 1、2 から総アクセス数と属性判別不能なデータを除外した、各属性別のアクセス動向をグラフ 3、4 に示す。なお、I 社は人数が少ないため、個人のアクセス動向が出やすくグラフの動きが平均化されず動きが大きくなっている。

これらのグラフから読み取ることは、ネットワーク利用のトラフィックの中で Web を利用した情報収集の比率が高いことにある。I 社および N 社においても、検索エンジン（属性名 search）、ニュースサイト（属性名 news）が多く、これらのサイトを利用したときに自動表示されるバナー広告等の付随アクセス（属性名 ad）これらと同じ変化を示して大きい。この 3 つの属性が Web トラフィックにおける大きな割合を占めている。



グラフ 3: 各属性別のアクセス動向（小規模企業 I）



グラフ 4: 各属性別のアクセス動向（中規模企業 N）

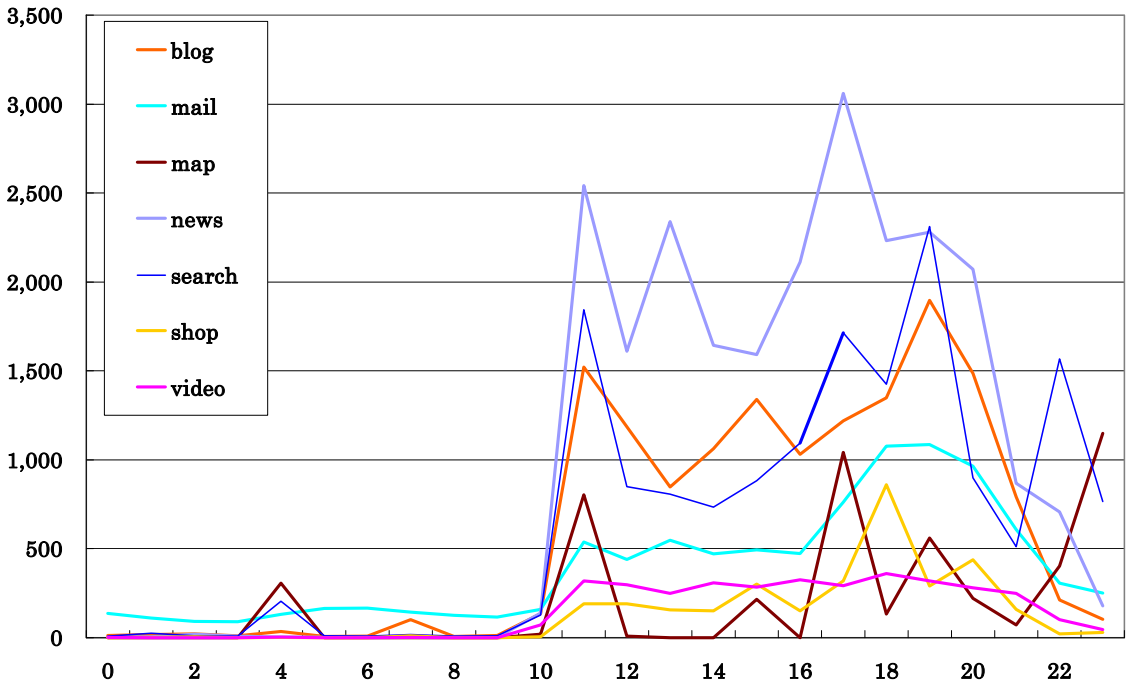
3.3 業務範囲内と業務範囲外のアクセスに関する考察

さらに業務範囲内と範囲外のアクセスに関して考察する。そのために、検索エンジンやニュースサイトと連動して自動的にトラフィックが発生する広告サイト（属性ad)、アクセス解析（属性analysis）、ソフトウェア関連のアクセス（属性app）も少ないので除外したアクセス動向をグラフ5、6に示す。

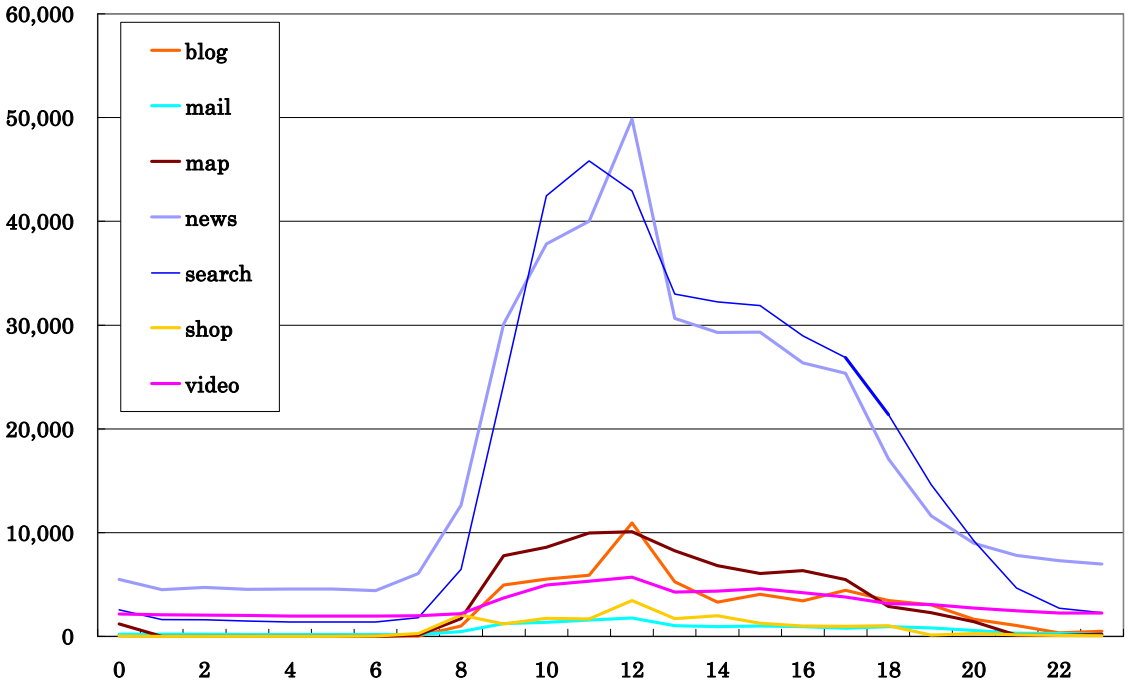
業務外のアクセスと考えられるのはブログ SNS サイトへのアクセス（属性名 blog)、ショッピングサイト（属性名 shop）はその可能性が高い。ブログによっては業務上の有用な情報が掲載されている可能性もあるが、その比率はそれほど高くないと考えられる。メール（属性名 mail）については、通常の電子メールではなく、Web ベースのメールサービス（Web メール）に該当する。

利用するとすればプライベートなメールの利用であるが、実際 N 社においてはアクセスが非常に少ないため無視して良いと考える。I 社においては Web メールの使用を禁止しておらず、アルバイトが業務で利用していることもあるので例外と考えて良い。

ここでポイントとなるのが、検索エンジン（属性名 search）、ニュースサイト（属性名 news）の扱いである。情報提供という意味では、地図サイト（属性 map）についても同様の位置づけと考えられる。これらのサイトの利用が業務範囲内外か判断することは一見難しいように思われるが、検索結果から実際のサイトに移動する際にリスエストが発生する



グラフ 5：主要な属性別のアクセス動向（小規模企業 I）



グラフ 6：主要な属性別のアクセス動向（中規模企業 N）

ので、業務範囲外の検索エンジン利用が多ければ前述の業務外アクセスも比例して増えることに

なる。これは、ニュースサイトでも地図サイトでも同じと考えられる。つまり、これらのサイトへのアクセスは主に純粋な情報収集のために行われていると考えて良い

次に時間帯での変化について検討を行う。Web 全体のトラフィックから企業の活動時間帯についても知ることができることはすでに述べたが、両社ともアクセスの立ち上がり後すぐに一度ピークを迎える。このピークが検索エンジン（属性名 search)、ニュースサイト（属性名 news）によるところが大きいが、出社後まず情報収集をするといった、ごく当たり前の行為が行われていることが確認できる。

業務範囲外のアクセスに注目すると、特に N 社では昼休み時間帯に微増していることが確認できる。また、I 社においても時間が遅くなれば増える傾向にあり、日中時間帯に業務範囲外のアクセスを行っているという事実は確認できない。

3.4 考察

今回、特にアクセス制限が行われていない小規模企業 I（10 人規模）と、厳しいセキュリティポリシーを適用していない中規模企業 N（100 人規模）を対象とした。これらの企業は、最初に述べた「ともすれば画一的なガイドラインの遵守を強制的に職場に押し付けるものが多く、組織における一つひとつの職場の実態を考慮していない」といった国内の一般的企業とは異なる。しかしながら、特に厳しいセキュリティポリシーを適用しなくても、
業務範囲外のアクセスが多くなるわけではないという結果を示唆している。

むしろ、適度にコミュニケーションツールが利用されており、それは業務時間外に増えるといった、性善説的な行動が観測でき、ソーシャル・キャピタル充実の方向がうまくいっている例といえるのではないだろうか。

中小企業においても、IT 技術に明るくない企業であればコストをかけて画一的なセキュリティポリシーを適用しようと努力をしている可能性はあるが、今回の調査対象となったこれらの企業は IT 技術系である。これは、セキュリティ対策を行っていないのではなく、不要なアクセス制限がむしろ、業務に支障をきたすといったポリシーに基づき運用されている結果ととらえることができる。

4 アクセス制限がもたらす悪いユーザ動向

厳しいアクセス制限が、必ずしも、個人の行動の抑制に効果的に働くとは限らない。江崎らはトラフィックの観点でユーザ動向を分析している[23]。その中で、インターネットにおける利用プロトコルとポートの時間的変遷について調査を行っている。

4.1 ポート利用の変遷に関する調査

インターネットにおいて、データを交換する主なプロトコルがTCP/IPである。TCP/IPにおいては、IPアドレスによって通信相手を指定するが（IP層、OSIにおけるネットワーク層)、通信相手が提供している複数のサービスのひとつ指定するために、ポート番号を用いる（TCP・UDP層、OSIにおけるトランスポート層)。指定できる番号の範囲はTCPやUDPなどの通信の種類毎にそれぞれ 0 から 65535（16ビット符号無し整数）と定められている[24]。 これらの番号と、TCPやUDPなどの通信プロトコルの指定の組み合わせで特定される、論理的な通信の口をポートと呼ぶ。

利用されるポートとして代表といれるのがWebの80番である。Webサービスも SSLを利用する際には443番を利用する。このほか、メールの転送25番、受信が110番、名前解決に利用するドメインサービス（DNS）が53番となっている。また0番から1023番については、well-knownポートと呼ばれ、広く一般に供するサーバでの利用が推奨されている。

江崎らの調査では、2005 年と 2008 年おけるユーザが利用するポートに関するトラフィック調査を行った。ポートをよく使われる順に並べた結果が表 1 である。

問題としているのが、P2P（Peer to Peer）などのアクセスが、一見減っているように見えるが、そうではなく、ただみえにくくなっただけとしている点である。実際Winnyで利用するポート7743だけをとってみても、2005年から2008年では減少しているかのように見える。しかしこれは逆で、Winnyが問題とされることによって、それが分散して隠れてしまったということである。

---

[23] Kenjiro Cho, Kensuke Fukuda, Hiroshi Esaki and Akira Kato. Observing Slow Crustal Movement in Residential User Traffic. ACM CoNEXT 2008. Madrid, Spain. Dec. 2008.

[24] http://www.iana.org/assignments/port-numbers

protocol port	2005 total (%)	2005 client type	2005 peer type	2008 total (%)	2008 client type	2008 peer type
TCP *	**97.43**	**94.93**	**97.66**	**96.00**	**95.51**	**96.06**
(< 1024)	*13.99*	*58.93*	*8.66*	*17.98*	*76.16*	*11.35*
80 (http)	9.32	50.78	5.54	14.06	64.96	8.26
554 (rtsp)	0.38	2.44	0.19	1.36	8.21	0.58
443 (https)	0.30	1.45	0.19	0.58	1.63	0.46
20 (ftp-data)	0.93	1.25	0.90	0.24	0.17	0.25
81 (-)	0.15	0.04	0.16	0.23	0.04	0.25
82 (-)	0.05	0.01	0.06	0.19	0.01	0.21
110 (pop3)	0.17	1.00	0.10	0.14	0.46	0.10
22 (ssh)	0.09	0.17	0.10	0.10	0.16	0.09
25 (smtp)	0.14	0.51	0.11	0.07	0.11	0.07
1000 (-)	0.03	0.02	0.04	0.07	0.01	0.08
others	2.52	1.26	1.27	0.94	0.40	1.00
(>= 1024)	*83.44*	*36.00*	*89.00*	*78.02*	*19.35*	*84.71*
6346 (gnutella)	0.92	0.84	0.93	0.94	0.67	0.97
6699 (winmx)	1.40	1.14	1.43	0.68	0.24	0.73
7743 (winny)	0.48	0.15	0.51	0.30	0.04	0.33
1935 (rtmp)	0.20	0.81	0.14	0.22	0.73	0.16
6881 (bittorrent)	0.25	0.06	0.27	0.22	0.02	0.24
7144 (-)	-	0.02	0.03	0.19	0.03	0.21
8080 (-)	0.11	0.15	0.14	0.11	0.09	0.15
4662 (edonkey)	0.12	0.02	0.13	0.13	0.00	0.14
11560 (-)	0.03	0.02	0.10	0.04	0.01	0.11
3074 (-)	0.02	0.03	0.10	0.02	0.32	0.07
others	79.91	32.76	85.22	75.17	17.20	81.60
UDP *	**1.38**	**3.41**	**1.19**	**1.94**	**2.50**	**1.88**
53 (dns)	0.03	0.14	0.02	0.04	0.12	0.03
others	1.35	3.27	1.17	1.90	2.38	1.85
ESP	**1.09**	**1.35**	**1.06**	**1.93**	**1.85**	**1.94**
GRE	**0.07**	**0.12**	**0.06**	**0.09**	**0.08**	**0.09**
ICMP	**0.01**	**0.05**	**0.01**	**0.02**	**0.05**	**0.02**
others	**0.02**	**0.14**	**0.02**	**0.02**	**0.01**	**0.01**

表 1: インターネットにおける利用ポートの変遷

また 80 番ポートのアクセスが増えているがこれは動画サイトなどのリッチメディアコンテンツが増えたためとしている。これは、554 番のRTSP (Real Time Streaming Protocol) [25]の増加からも観測できるが、これらの一般的なポートのトラフィックに紛れ込んで、他のサービスが使われていることも示唆している。

この調査では、すでにポート番号でユーザがどのサービスを利用しているかを知ることはできなくなったと述べている。

4.2 制限が問題を分かりにくく、逸脱行為を増やす

ファイヤウォールをはじめとするネットワークトラフィック制御を行う機器の普及により、不要なポートやアクセスを制限することが一般的に行われている。厳密なセキュリティポリシーを適用している企業においては、プロトコルとポートの利用が厳しく制限され利用できるネットワークアクセスが限られることになる。

そこで不便を感じたユーザは、抜け道へと走ることになる。すでにポート番号でユーザがどのサービスを利用しているかを知ることはできなくなったという事実は、むしろ正規でないアクセストラフィックを増大させていることを示している。これは、厳しい規制が否定的な組織感情を生み、その結果逸脱行為を行わせる動機となりうることを示唆している。例えば、たびたび社会

[25] http://tools.ietf.org/html/rfc2326

的問題となる、企業内におけるWinnyの利用はその典型例と考えられる。

5 調査結果総括

本調査は、企業活動に伴って必ずネットワークを介した情報交換が発生する点に着目し、企業ネットワークに流れるトラフィックを観測することで、ネットワークに流通する情報と企業活動との関連性を調査した。画一的で厳しいセキュリティガイドラインの遵守が企業ガバナンスにおいて必ずしも適切ではいという疑問を投げかけたい。

トラフィック分析による結果として以下が言える

- 特に厳しいセキュリティポリシーを適用しなくても、必ずしも業務範囲外のアクセスが多くなるわけではない。むしろ、適度にコミュニケーションツールが利用されており、それは業務時間外に増えるといった、性善説的な行動が観測できる。
- ネットワーク利用に厳しい制限を与えることで、正規でないアクセストラフィックを増大させている。制限がなければ検出できる行動が、制限を当たることで逆に検出が難しくなっているというねじれが発生している。
- さらに、厳しい規制が否定的な組織感情を生み、その結果逸脱行為を行わせる動機となりうる（e.g. P2Pソフトウェアによる情報漏洩問題）

これは「1.2 画一的で厳しいセキュリティポリシーの弊害」で取り上げたユーザの意識調査の結果と、実際のユーザの行動であるネットワークトラフィックの分析結果が、一致していることを意味している。その点を考慮すると、

「締め付けによる否定的な組織感情と情報セキュリティ対策に対する否定的な意識が、問題を分かりにくくするとともに、逸脱行為を誘発する」

といえる。逆に言えば、

「適切に厳しくないセキュリティポリシーを適用することで、ソーシャル・キャピタルの充実に貢献でき、結果的に業務効率や逸脱行為が減る」

という仮説を立てることも可能となる。

インターネットは企業の業務活動に必要不可欠である以上、利用者が否定的な組織感情を持たない範囲で安全な運用ができることが理想である。そのためには、

- 画一的で厳しいセキュリティポリシーの弊害を認識する必要がある。否定的な組織感情が強くなれば自然と逸脱行為に流れる可能性がある。
- インターネット利用の制限と否定的な組織感情が業務の効率を下げる。
- 各組織に見合ったセキュリティポリシーの制定し不必要な制限を避けるべき。
- 制限はしないが監視を怠らず、逸脱行為の防止もしくは、発生時の責任の所在を明確化する運用を行うべきである。

といった見直しが、企業ガバナンスにとって必要と思われる。

一方、画一的で厳しいセキュリティガイドラインの遵守が企業にとって見ればリスクの最小化である。上記のような前提に基づいて企業がガイドラインを作成した場合、職場環境の向上につながるかもしれないが、逆に個人の資質に頼ることなり、少数の悪質な個人のリスクを企業が回避しずらくなるという問題も考えられる。そのため、この問題は責任制度とセットにして行う必要があると考える。

第 4 編　個別提言

1　ガバナンスのあり方に関する提言

1.1　外部委託と情報セキュリティ対策に関する提言(佐藤)

【背景及び問題点】

組織における情報セキュリティ対策において、常に難題のひとつになっているのが外部委託における機密保護対策である。その背景には、外部委託の対象となる業務様態が広いことがあるが、これを一意に検討すると具体性を欠くことになる。また、外部委託の問題を考えるときに、委託先に課すべき義務のみだけに着目し、委託元の義務すべきことを曖昧にしたり軽減しようとしたりする点がもう 1 つの背景として考えられる。

その代表例が、委託先に対して ISMS 認証やプライバシーマーク認証の取得を単に求めるような行為である。ISMS 認証については、認証取得の取得対象部門の範囲と内容は適用宣言書で特定されている。委託先の情報セキュリティ対策状況を確認するための質問票に、「貴社は ISMS 認証を取得しているか？」という項目を入れる場合があるが、ISMS 認証は部門単位であり、「会社が認証取得している」という表現をすることは、そもそも禁止されている。それに相当する適切な表現は、「全部門が認証取得している」となるが、委託した業務を実施する部門と関係ない部門に対しても認証取得を要求していることになる。また、ISMS 認証は情報セキュリティ対策のレベルを一定に保つものではない。リスク評価に基づいて適切なリスク対応をするというマネジメントシステムが構築されていることが認証の対象である。言い換えると、リスク対応としての対策レベルを低くして、高いリスクがあるとしても、それを認識・評価した上で受容するという判断をしているのであれば、対策レベルは低いままでも認証の取得は不可能ではない。そのため、上記の質問は注意深く行わないと意味がなくなる。一方、プライバシーマークの場合、取得は法人単位で行われるが、適用対象の選択が可能である。例えば、個人情報を含むデータ保存に関する業務について、プライバシーマーク取得している事業者が委託元として、同マーク取得しているデータセンターに外部委託を行う場合があったとする。この場合、委託元は、自社ではデータ保存を実施していないことを理由に認証取得の範囲外とすることができ、委託先は、データの内容は委託先のみが知り得るものであって、自社の個人情報ではないことを理由に、範囲外とすることができる。その結果、個人情報を含むデータは、両者ともにプライバシーマークの対象外となる事態が起こり得る。

こうした例からわかるとおり、委託元が委託先に、ISMS 又はプライバシーマーク認証取得を単純に求めるだけでは不十分となり得る点に注意しなければならない。また、認証取得部門や業務、対象情報の範囲を個別に指定したとしても、認証取得は委託発注前の実績を問うものであり、既に存在する業務手順とこれから発注する業務手順の相違による影響を踏まえなければならない。

以上のことから、外部委託における情報セキュリティ対策は、これから発注する委託業務においてどのような対策を講ずるのかを明確にするとともに、外部委託の業務をいくつかの観点で細分化して、それぞれの特徴を踏まえた上で課題を整理することが必要である。

そこで、この提言では、以上の背景及び問題点に留意しつつ、外部委託における情報セキュリティ対策の課題整理及び改善のための提言を行う[26]。

【検討事項・視点】

(1)　委託契約の性質(派遣か請負か←How)

委託契約の場合における情報セキュリティ対策の観点から重要なことは、作業員が派遣であるか請負であるかの違いである。派遣の場合は、日常的な業務作業の指示及び監督が委託元にあるため、情報セキュリティ対策の指示及び監督は委託元とするのが現実的である。請負の場合は、委託元が委託先の作業者に直接作業指示をすることは法律上認められていないため、情報セキュリティ対策についても委託先が最終的に指示せざるを得ない。ただし、委託元は、作業者個人ではなく委託先企業に対し、必要な対策を指示することはできる。ただし、指示していない対策についてまで、委託先が必要に応じて適宜補完することを要求することは、委託元の利己的な行為であるため適切ではない。

[26] 本提言では、機密性の保護に焦点を絞って取り上げる。

委託元の作業場所で委託業務を実施する請負業務では、偽装請負との関係で問題となる場合がある。実質は、委託元が作業者に日々の作業指示を行っている場合は、情報セキュリティ対策の指示も委託元が行うのが現実的である。それにもかかわらず、契約形態が請負であることを理由に対策指示を曖昧にするといった本末転倒を回避するため、契約形態を実態に正す必要がある。

(2)　委託業務の実施場所(委託元か委託先か←Where)

委託元作業場所で請負業務を実施させる場合には、物理的(施設的) 情報セキュリティ対策は、委託元が行うよりほかはない。社員に対する十分な対策が、非社員に対しても有効であるか否かのリスク評価は委託元の責任である。その対策が不十分であるにもかかわらず、委託先社員が事故を起こした時に、請負であることを根拠に委託先に責任を一方的に問うのは適当ではない。

(3)　保証の内容(注意義務か結果責任か←When)

委託元としては、特段の具体的対策を指示することなく事故が起きないという結果を、委託先に保証させることを期待したいであろう。一方の委託先は、受注時点で顕在化していない脅威への対策を講じることを見積もることはできず、ましてや事故により生じる予測不能な損害賠償を保証することは現実的ではないと考えるであろう。

現実的な範囲で考えるのであれば、委託元が委託先に対して、情報セキュリティ対策として講じるべき注意義務を明示することで、委託先の不備があれば債務不履行責任を問い、委託元の指示内容に不足があれば、委託先への全責任を問えないことになる。このことは、一見、委託元にとって不利のようであるが、それは事後的な金銭賠償でしか担保されない結果責任を求めるよりは、事故を未然に防ぐための対策を講じることの利益に着目すべきである。結果責任を偏重すれば、委託先は、予防対策よりもむしろ、保険加入などに対策原資を割り当てるという経済原理が働き得ることも憂慮するべきである。

したがって、委託先において必要となる対策は、外部委託を行わない場合を仮定したリスク評価と対応を検討し、講じるべき対策を自ら決定し、それを委託先に示すことが基本である。

(4)　リスク評価の主体(業務専門性を有するのが委託先か委託元か←Who)

リスク評価と対応選択に基づき情報セキュリティ対策を決定して指示するのは、原則として委託元である。ただし、委託元において、委託業務の専門知識を有していない場合は、委託先が一連セキュリティ対策を実施する方が、効果的である。この場合は、委託元は、委託業務の実施能力を評価するのと同様、情報セキュリティ対策の実施能力を評価することに手間をかける必要がある。

(5)　取り扱うデータの種類の検討(個人情報を取り扱うソフトウェア開発の例←What)

委託業務の種類は多種多様であり、それぞれに特定するリスクを検討しなければならないが、ここではITシステムのソフトウェア開発の際に個人情報を取り扱う場合において、日本固有の問題があることを例にあげる。

ソフトウェア開発の検収時の受入検査では、テストデータが必要となるが、個人情報を処理するソフトウェアの場合には、テスト用の個人情報が必要になる。この時、実際の個人情報をテストに用いることは、情報セキュリティ対策として好ましくないが、ソフトウェアの受入検査としては品質確認の精度を高めるのに役立つ。このことは、アルファベット文字しかない欧米では、容易にテストデータを生成できるのに対して、外字や名寄せ、文字コードの問題を持つ日本では、実際の個人情報を使うより確実なことはないという違いがある。

委託元企業にとっては、実際の個人情報を用いることは望ましくないが、委託先側のみでなく委託元担当者にとってはメリットがある。なぜなら、テストデータを使って受入検査を合格させた後に、実際の個人情報でソフトウェアの不具合が生じた場合には、受入検査の委託元担当者の責任が問われかねないからだ。

この問題を解決するためには、日本語特有のテスト用の個人データが、工業標準規格などのような第三者的な立場で用意され、それを用いたテストによれば、委託元担当者と委託先の双方の責任が軽減される必要がある。委託元企業は、決定した対策が、委託先ばかりではなく、自社の委託発注担当者にとっても過度の負担になっていないかを十分注意する必要がある。

(6)　対策実施者(←Who)

外部委託の情報セキュリティ対策を考える場合、対策の実施者が委託先に限られるかのような錯覚が生じやすい。しかし、保護すべき情報は委託元の情報であることから、第一次的な対策実施者は委託元であると考えるのが自然である。委託業務にとって必要最小限の情報だけに使用を制限するのは、委託元の責任である。したがって、外部委託の情報セキュリティ対策は、委託元

と委託先双方で実現しなければならない。

【提言】
以上の認識に基づき、外部委託における情報セキュリティ対策の改善としては、次のような提言を行うことができる。
①派遣と請負は実態に即して区別した上で、派遣業務については、委託元が情報セキュリティ対策の責任を持つべきである。
②作業場所についての物理的(施設的)情報セキュリティ対策の責任は、派遣か請負かや、委託元か委託先かにかかわらず、その場所の所管者が持つべきである。
③リスク評価、対応選択、対策決定については、結果責任を偏重することなく、委託元が委託先に具体的に指示することを基本にするべきである。ただし、請負業務において、業務の専門性を委託元が有していない場合に限り、委託先にセキュリティ対策を依頼することができる。その場合にも、結果責任を求めすぎるあまり、リスク軽減としての未然防止ではなく、対応選択としてリスク転嫁選択されないように注意すべきである。
④委託元は、自社が実施すべき対策についても予め委託先に対して明示すべきである。委託元がかかる義務に違反している場合に、委託先が当該事実を報告又は相談しやすいような環境整備をすべきである。
⑤外部委託において、委託先の ISMS やプライバシーマーク認証の取得の有無を参考にする場合には、認証対象範囲に注意しなければならない。委託する業務と無関係の業務については、無意味な確認か過剰な要求になるからである。また、委託する業務が委託先にとっての定型業務ではない場合には、業務を委託するより前の時点での認証取得の効果についても注意すべきである。
⑥請負業務において、個人情報を含むソフトウェア開発を委託する場合であって、実際の個人情報をテストに使わない場合は、テストデータの標準化が期待される。さらには、外部委託に限らない問題ではあるが、同一の日本語に対して複数の日本語コード体系を併用しているという特異な状態を改善することも、動作確認に実際の個人情報を用いるという悪慣習の是正には一助になるものと考えられる。

1.2　アジア地域に進出している日本企業の情報セキュリティマネジメントの現状と取組みの改善(早貸)

【背景】
我が国の少子高齢社会化による国内市場の縮小と労働人口の減少や、世界的なコストダウン競争の加速により、アジア地域各国への製造拠点の移設や現地の労働力の活用による生産コストの削減や、現地市場の開拓（市場に応じた製品投入のための研究開発センターを現地に設置する等の活動を含む。）の必要性は日に日に高まっていると言える。このような事情を背景に、日本企業のアジア地域各国への進出や現地企業へのアウトソーシング等、域内各国と我が国の経済的結び付きは年々強くなってきている。
日本企業が進出先またはアウトソーシング先の選定を行うにあたっては、その国または地域の治安や重要インフラの安定度等、様々な選択要因があるが、技術情報等の知見や経験に関する情報を展開するためには、進出先における情報セキュリティマネジメントのレベルは重要な問題となる。　また、アジア地域各国におけるインターネットや IT 技術の利用拡大に伴い、域内各国と我が国との間の経済活動の IT 依存度も高まっており、ひとつの国で発生した情報セキュリティインシデントが他国に波及し、域内の社会経済活動に被害が拡大するリスクも高まっているといえる。
このような状況から、各国の社会経済活動の継続性や円滑な経済連携を維持するため、アジア地域にセキュアな IT 環境を構築するための国際協力、連携の重要性が認識されており、セキュリティ水準の向上等の環境整備のための様々な官民による支援活動も展開されているところである。
【日・ASEAN 情報セキュリティ政策会議】
本年２月には、日本並びにＡＳＥＡＮ加盟国１０ヶ国の経済・投資関係省庁及び情報通信省庁の高級事務レベル（局長・審議官クラス)、ＡＳＥＡＮ事務局、日本経済団体連合会、電気通信事業者、情報セキュリティ関連機関及びその他の民間企業等が参加して、「第１回日・ＡＳＥＡＮ情報セキュリティ政策会議」が開催され、①ＡＳＥＡＮに進出する日系企業が安全に情報

をやり取りできるセキュアなビジネス環境の構築を実現すること、②企業活動を支える根幹となる情報通信インフラの安全・信頼性の向上に向けた取組みを推進すること、③事前予防策、事後対応策を含めた情報セキュリティ対策の国家戦略の充実に向けた取組みを推進することを目的として、意見交換が行われた。

①の「知識社会におけるセキュアなビジネス環境整備」に関するセッションにおいては、経済産業省から「技術情報（製品に関する情報、知的財産等）、個人（顧客）情報の漏洩に関するリスクが高まってきており、情報セキュリティ対策の実効性を確保するためには、技術的な解決策に留まらず、企業のガバナンスを視野に入れた包括的な対策が必要である」旨のプレゼンテーションが行われ、ＥＲＩＡ（東アジア・アセアン経済研究センター）での政策研究、コンピュータセキュリティに関する緊急時対応体制の整備、情報セキュリティマネジメントシステム（ＩＳＭＳ）の普及促進、ＡＳＥＡＮ各国の人材育成やセミナーの開催といった日本の施策が紹介された。

また、日本側の産業界からは、ＡＳＥＡＮ各国での事業展開に際して、情報セキュリティが重要な要件の一つとなる旨の紹介があり、「知識集約型産業、高付加価値産業の成長を通じて知識経済化が進むアジア諸国において、技術移転・知識移転の必要条件となる情報セキュリティ対策を実施していくことの重要性の認識」が共有された。

（参照：http://www.nisc.go.jp/press/pdf/aseanj_conference2009_press.pdf）

【我が国の視点、アジア諸国の視点】

以上のとおり、我が国のアジア諸国に対する情報セキュリティ施策は、「高度な情報セキュリティ対策が対外直接投資やアウトソーシング等を活性化する」（投資を得るためには、情報セキュリティ対策の推進が必要）との視点を吸引力として、アジア地域各国内の産業界における情報セキュリティ意識の向上を図るための取組みを進めるというものであり、基本的なスタンスは、我が国においては一定レベルの情報セキュリティマネジメントの導入、実施が進んでいることを前提に、そのモデルを、ASEAN を中心とするアジア地域に持ち込んで浸透を図ることにより、我が国企業のアジア地域における活動の円滑化を図ろうとするものであるといえる。

アジア諸国と一言で言っても、情報セキュリティ対策の実施の状況については、国ごとに大きな差異があるが、総じて言えることとしては、ASEAN 諸国においては、シンガポール及びマレーシアの政府機関及び大企業を除き、情報セキュリティ意識は必ずしも高くなく、適切な情報セキュリティ対策が実施されていない傾向にある。特に、機密情報、重要情報に関する管理・保護意識は、雇用側従業員側ともに低く、それらの情報が漏えいしている可能性もしくは漏洩の事実に気がつかない可能性は否定できない。また、経済格差により正規のソフトウェアの価格が高額になってしまうことから、正規ソフトを購入する習慣がなく、違法コピーソフトの利用が当然のことのようになってしまっているため、セキュリティ問題に対する修正プログラムをあてることができず、結果的にウイルス感染が避けられない環境も問題となっている。

このような状況を改善すべく、「海外の投資を呼び込むためには、情報セキュリティ対策、マネジメントに対する配慮が必要である」ことについての理解を求め、各国内の情報セキュリティマネジメントレベルを向上させるというのが、上記の我が国の施策であるが、具体的に浸透を図ろうとする日本モデルの具体的な内容については、検討が必要であろう。

実際に、アジア各国の企業やコンピュータセキュリティに係る緊急対応チーム等の担当者の声としては、海外からの投資には強い関心があるが、必ずしも日本からの投資のみを期待しているわけではなく、米国、EU, 中国等、取引比率的には日本と同等以上の国、地域が存在していることを前提にせざるをえないので、日本企業独自のスタンダードではなく、グローバルスタンダードに適合する形での情報セキュリティ対策の実装を図りたいと考えているとの意見が多い。

この問題は、国内において、大企業が中小企業に対して情報処理その他の業務を委託する契約等を締結する場合において、中小企業側が複数の大企業と取り引きしようとすると、発注元ごとに異なる情報セキュリティ対策等の要請に応えなければならず苦慮している実態があるという問題を解決しないまま（すなわち、統一された「日本モデル」が確立できていない状況のまま）、アジア地域のアウトソーシング先に対して「日本モデル」の情報セキュリティ対策の実装を求めようとしているようにも見え、実施レベルでの実効性に対する懸念が否定できないところである。

さらには、「現地に進出している日本企業」の実態に関し、必ずしも、情報セキュリティ意識

が高くなく、適切な対策が実施されていないのではないかとの声も少なくなく、日本モデルの導入が本当に情報セキュリティ対策として有効であるとの実感を得ることは難しいとの現地セキュリティ機関の意見もあるところである。実際、現地に進出している日本企業について、「現地の日本人経営者が情報セキュリティに関心がなく、情報セキュリティ対策を現地スタッフ任せにすることが多い（違法コピーソフトを使用している等の実態を日本人経営者は把握していないことが多い。）。」「現地日本企業と取引をする際にも、情報セキュリティ対策等に関する仕様や条件を提示されることはあまりない。」といったコメントをよく聞く。

すなわち、アジア地域に進出している日本企業における情報セキュリティ上の問題は、現地各国の情報セキュリティ対策、政策以前の問題として、現地の実情に合致した情報セキュリティ対策を実行しない日本側の経営のあり方自体が抱えている問題であるとの見解が根強い。

【検討が必要となる事項】

・アウトソーシングの場合

国内外の企業等に対するアウトソーシングに関する情報セキュリティ対策については、本年6月に、経済産業省から「アウトソーシングに関する情報セキュリティ対策ガイダンス」が公開されている。

（http://www.meti.go.jp/press/20090630007/20090630007-4.pdf　）

本ガイドラインにおいては、事業戦略に基づき、アウトソーシング戦略と情報セキュリティ戦略との整合性をとりながら、アウトソーシングにおける情報セキュリティ管理基盤を整備した上で、アウトソーシング先の選定や契約内容の検討、業務の実施状況の確認等の実行・評価プロセスや、社内プロセスの改善、アウトソーシング先の情報セキュリティ水準の向上等の改善プロセスを実施すべきことが言及されており、それぞれの実施事項におけるリスクと実施上のポイントが整理されている。また、特に、海外へのアウトソーシングを行う場合のリスク及び対策の方向性として、(1)高い離職率によるリスク（提供した情報は流出することを前提とする）、(2)文化や価値観の違いによるリスク（安全に係る意識の差が大きくセキュリティ要求の意図が伝わらない）、（３）コンプライアンスのリスク（暗号規制、知財保護の対象の相違等）、（４）自然災害、疫病、テロ・戦争等のリスク（事業継続計画の必要性）、（５）委託業務の高度化によるリスク（より高度な業務を委託する場合には、提供する情報の範囲も拡大するので情報のアクセス権管理の強化が必要）等への言及があり、このようなリスクについてアセスメントを行い、対策の加除修正が必要かどうかの判断を行うべきであるとされている。

これらは、アジア地域の企業等に対するアウトソーシングに関しても、あてはまるところであるが、情報の機密性や重要性に関する認識の大きなずれや違法コピーソフトの利用等、上述のような日本国内とは異なる地域的リスクを踏まえた上で、アウトソーシング先の選定や相手先に求める対策の内容を検討すべきであり、これらの検討に当たっては、現地の状況（法制度面のみならず、ネットワーク、ハードウェア、ソフトウェア等の技術的環境を含む。）を適切に理解している者の関与を得ることが重要であるといえる。このような状況を踏まえない、日本国内における対策をそのまま現地企業に求めるような運用では、情報セキュリティ対策の実効性が確保できない可能性が高い。

とりわけ、現地における技術的環境については、変化が激しく、理解する上で、通常の取引慣行等の実態とは異なる技術的な知識が必要とされることから、これらの技術的環境に関する適切な助言を行うことができる現地組織との連携や、日本側の担当者の技術的な問題に関する知見のレベルアップ等が必要となるであろう。

また、アジア地域の各企業が、日本以外の国の企業からのアウトソーシングをも受けることを前提に活動をしているという実態を踏まえ、その国において普及している、運用上の、もしくは技術的なスタンダードと排他的関係に立つような対策の実施は、求めても実効性がないことを認識すべきであり、追加的に独自の対策を要求する場合には、情報セキュリティ対策に関する用語の意味する実質の確認や、対策の継続的な実施を確認するための評価方法等について、上述の地域的リスク等への配慮を行ったうえで、十分な合意形成を行う必要がある。

・現地法人

アジア地域に進出している日本企業における情報セキュリティ対策が必ずしも十分なレベルにないとの懸念については、「現地の日本人経営者が情報セキュリティに関心がなく、情報セキュリティ対策を現地スタッフ任せにすることが多い（違法コピーソフトを使用している等の実態を日本人経営者は把握していないことが多い。）。」「現地日本企業と取引をする際にも、情報

セキュリティ対策等に関する仕様や条件を提示されることはあまりない。」等のコメントに示されるとおりであり、現地に派遣されている日本人経営者の情報セキュリティに対する関心や知識の不足の問題が、そのまま、その日本企業の情報セキュリティ上の脅威の源になっているといえる状況は、当該日本企業にとって問題であるばかりでなく、その企業との間で取引等を行う現地企業等にとっても不安材料となり得る。

現地法人についても、アウトソーシングの場合と同様、地域的リスクに対応すべく、現地の法制度面や、ネットワーク、ハードウェア、ソフトウェア等の技術的環境に関する適切な認識、理解に基づいた（追加的な対策が盛り込まれた）セキュリティ基盤の構築、運用を行うことが必須であると言える。日本人社員等の現地経営層に情報セキュリティに関する専門的な知識を要求することは必ずしも現実的ではないが、少なくとも、そのような事実や状況について現地経営層に十分な教育を行った上で、日本側の情報セキュリティ担当者との十分な情報連携体制の構築、維持、及び、現地の技術的環境や運用の実態に関する助言を得ることができる現地組織等との連携協力関係の構築等を進める必要がある。さらには、「現地法人等の拠点を海外に置く場合には、これら情報セキュリティ対策に関する配慮が不可欠であること」を日本側の経営層が適切に認識（現地に派遣する者を選定する段階における配慮等においても。）することが重要であるといえる。

・セキュアなビジネス環境構築の支援

冒頭に述べたとおり、アジア地域に対するアウトソーシングや現地進出を行う企業の活動を支援するという観点から、アジア地域におけるセキュアなビジネス環境を構築する官民の取組みが進められているところであるが、それらの取組みにおいても、現地の制度的、技術的な実情に即した情報セキュリティ対策のあり方や、アジア地域に進出している日本企業における情報セキュリティマネジメントの実態（「相手先国における情報セキュリティ政策上の対応を奨励する等より前に、まずは日本から現地進出している企業自身における取組みの改善からではないか」等との反応）をも十分に考慮に入れた上で支援活動の具体的内容が検討されるべきであろう。

1.3 情報セキュリティ・ガバナンスにおける内部統制規制のあり方(柿崎)

【提言の目的】

今日の IT 社会における企業内の情報保護については、「情報」という規制対象の性質の特殊性に着目した管理体制とその法規制が求められている。もとより、企業内部では、営業上のノウハウ等の企業秘密に属する情報や、顧客に関する個人情報が集積されている。これらの情報は適切な手続なしに公開されるべきものではない。他方で、企業の財務情報などの一定の企業情報は、資本市場における投資家らの投資判断の基礎とされるものであるから、それらの情報は適時・適切に開示されなければならない。しかし、こうした情報が、適切な手続なしに企業外部に漏えいした場合、あるいは虚偽の企業情報が市場に開示された場合には、今日の IT 社会においては、不特定多数へコストレス、タイムレスで伝搬し、予測を超えた被害をもたらす恐れがある。こうした損害について、事後的救済により被害者の特定や損害額の算定を正確に行うことは、今日、極めて難しい状況にあるといえる。したがって、情報セキュリティに関するリスク・マネジメントは、事後的救済とともにリスクが顕在化する前の予防的対応に主眼をおいた企業における情報管理のあり方が問われることになる。それと同時に、そうした情報管理の整備が企業にとって業務の効率性をあげ、訴訟リスクの回避にも貢献できるような法制度の設計を提案することが必要であろう。そこで、こうした予防的情報管理の手法として、IT 統制を内包した内部統制のあり方が、今後のリスク・マネジメントの欠如に対するひとつの打開策となる可能性がある。その方法論として、既存の法体系（ここでは金融商品取引法・会社法）の責任の枠組み（ハード・ロー）に基盤を置きつつ、これを補完するソフト・ローとしての具体的な自主ルールとの連携により、内部統制構築、評価、監査、開示を確保する実効性ある法執行システムのグランド・デザインの方向性を提言したい。

【米国の SOX 法に基づく内部統制規制とその運用】

わが国での内部統制規制のあり方を検討する前提として、まず研究対象としたのは、内部統制規制につき先行する米国 SOX 法規定とその運用についてである。米国においては、2002 年 SOX 法に基づく内部統制制度の導入により、上場企業の IT 統制を含む内部統制システムの整備が進行している。もとより SOX 法は、連邦レベルの資本市場規制法の一環として位置づけられてい

るため、公正な資本市場の機能の確保がその最終目的であり、その実現のためには、市場にリアルタイムで提供される情報の真実性を担保する企業のガバナンスの確保に向けた規制が必要とされる。さらに、高度に IT 化の進んだ今日の資本市場における情報コントロールは、単なる企業内部のオペレーショナル・リスク等に対処するものでは足りず、情報そのものの性質に着眼した市場全体のリスク・マネジメント体制と、それらに見合う責任を確保する法制度の整備が望まれている。

もっとも、こうした米国の SOX 法に基づく内部統制の整備を巡っては、導入当初、企業に過重な整備コストを負担させるのではという懸念があり、問題解決のアプローチとしての妥当性が疑問視される声も報道されたが、この点については、実証的な研究により、SOX 法上の内部統制規制導入による米国経済への負の影響はかなり限定的であり、むしろ企業内の内部統制整備が一巡した現段階では、業務の効率化にも貢献する体制として再評価されつつある。さらに現段階で適用が延期とされている小規模公開会社に対する内部統制監査についても、2010 年 6 月 15 日以降の事業年度より適用とされることとなった。小規模公開会社に対する内部統制制度の適用免除を求める声も高いが、SEC の最終的な判断としては、資本市場を活用する上場企業に共通する前提条件として、企業の財務報告の信頼性を担保する規制の適用をうけるべきであること、小規模公開会社の導入費用の問題よりも、これを導入しない場合の市場のシステミック・リスクの影響が懸念されることなどを理由として、すべての SEC 登録企業に対して内部統制監査を含めた内部統制規制の適用を求めることとなった。

では、具体的に米国の SOX 法内部統制規制違反に対して規制当局はどのような法執行をおこなっているのであろうか。この点、米国の SOX 法の運用にあたり、市場規制機関である SEC の対応は、内部統制上の問題点が顕在化する過程で、段階的なエンフォースメントのアプローチを採用している。第一段階として、非公式の予備調査が行われる時点では、SEC は決して問題情報を公にせず、調査対象企業の経営者、内部監査人、法務部長らと面談し、企業内部で早期に問題の解決と是正措置の導入を迫ることにより、正式な法執行手続き段階に移行しないまま対処する手法がとられている。第二段階として、おもに会計上の問題などの発覚を契機として、Form8-K（臨時報告書）や、Form10-Q（四半期報告書）に重要事項の開示を要求されるときに、内部統制は有効であるとの宣誓書がすでに添付されている場合には、問題が発覚しているのになぜ内部統制が有効と評価できるのかについて、スタッフ・コメント・レター(SEC Stuff Comment Letter)が送付され、問い合わせをうける場合がある。これに対して企業側は、応答書簡でその理由を開示するか、もしくは「開示統制・手続きが有効ではなかった」という四半期報告書のリステートメントを提出することになる。たとえば、臨時報告書では、監査人の辞任や解任を契機として、その理由をつけてこれを開示しなければならないが、経営者は、監査人の任期中に経営者との意見の不一致、または「内部統制上の重要な欠陥」や「著しい不備」があったならば、その監査人から監査委員会へ報告がなされるため、この点の説明を、スタッフ・レターで求められた事例がある。これを受けた企業は、その詳細な説明を応答書簡（Issuer Response Letter）で答えるか、臨時報告書のリステートメントを提出することになる。また、四半期報告書では、SOX 法 302 条に基づく「開示統制・手続き」が有効である旨の宣誓書の添付が求められているため、会計上の処理に不審な点があった場合、（たとえば収益の過大評価（overstatement of revenue)、会計操作（earning management）など）に、SEC は、このような会計上の問題があるにもかかわらず、四半期報告書に「開示統制・手続き」が有効であると結論付けた理由を開示せよ、というスタッフ・レターを送付する。これに対して企業側は、応答書簡でその理由について具体的に開示するか、もしくは、「開示統制・手続きが有効ではなかった」という四半期報告書のリステートメントを提出し、そのなかで内部統制上の重要な欠陥等を開示する場合もある。さらに 404 条の早期適用会社でない場合であっても、年次報告書において、内部統制上の重要な欠陥の指摘が監査人から期中にあった場合には、それを「事業リスク」として開示するか、なぜそれが、事業リスクとならないのか説明せよ、というスタッフ・レターが送付された場合もあった。大方の問題は、これらの臨時報告書、四半期報告書、年次報告書のリステートメントと SEC に対する応答書簡での説明という対応で処理されるようである。第三段階として、重大な違法性の問題を抱えた事例や、SEC との間で見解の相違をあくまで争うといった事例が、正式な SEC によるエンフォースメントの発動に発展していくことになる。すなわち、SEC による民事制裁金、排除措置命令、利益の吐き出し、取締役・執行役の就業禁止命令、などの多様な法執行が行われ、とくに重大な違法性が認められる場合には 1934 年

連邦証券取引所法 Rule10b-5 違反にも該当することも多く、さらには司法省による刑事訴追などへと繋がっている。
以上のようにSECの法執行のアプローチは、事前には予防的、柔軟、迅速な対応に焦点をおき、リスクが顕在化したのちは、将来の市場での不正の防止および原状回復、ならびに被害者救済の確保を目的とした厳格な対応がとられており、２つのアプローチが段階的に使い分けられている。もっとも現代の市場規制の目的は、民事責任や刑事責任を確保するハード・ローによる対応のみでは十分に実現できない状況にある。損害賠償責任を求める際に因果関係の立証を含め、厳格な要件の立証を課される被害者側の負担は、迅速な被害者救済の要請には生来的にそぐわない側面があり、また企業不正に対して刑事責任を安易に導入することは、犯罪の抑止効よりも経済活動の委縮を招く場合があるので慎重でなければならない。事後的救済においても、民事責任、刑事罰にとどまらない、柔軟で多様なエンフォースメント手段の整備（たとえば、被害者救済に民事制裁金・利益の吐き出しを活用する基金である Fair Fund の創設など）が求められている所以である。
したがって、情報の不可逆性に鑑みれば、一旦、市場にもたらされた虚偽情報については、現状回復による救済には限界があり、そこからもたらされる不特定多数への被害拡大防止の必要性から、事後救済を補完する再発防止の社内体制整備に向けられた一定の強制力の発動を伴う事前の有効な規制のあり方こそが、次の重要な課題といえる。
こうした米国での規制機関によるエンフォースメントに鑑みれば、我が国における内部統制規制を実効的に実現するエンフォースメントの手法がかなり貧弱であることを指摘せざるをえない。とりわけ、こうした市場の特徴を熟知した米国のエンフォースメントのあり方と比較すると、金融庁の硬直的で多様性に乏しい法執行手段では、市場規制機関としての目的を実現するには不適切なレベルにある。もっとも、この点については、現在、東京証券取引所などの現場レベルでの対応により補完される傾向にある。東証規則によれば、内部統制上に重要な欠陥がある場合にも、直ちに上場廃止というサンクションを用いるのではなく、特設注意市場への移行など段階を踏みながら、会社内部で是正手段を有効にとりうるエンフォースメントを実施している。さらに来年からは、内部統制の重要な欠陥が識別された時点で、資本市場への適時の開示が要求され、市場に対するリアルタイムでの内部統制の情報の提供が図られることになろう。ただし、東証ルールは、あくまで市場開設機関の自主ルールにすぎないため、金融庁の対応に必要な調査権限等を代替させるには限界がある。国家権力を背景とした市場監督機関による機動的な調査・監督・執行の手段の確保がより一層重要となるものと思われる。こうした内部統制規制のエンフォースメントに関しては、今後は、いわゆるソフト・ローとハード・ローの連携がさらに重要となり、会社法、金商法、東証規則等の内部統制規制の横断的運用の方向性については、それぞれの規制手段の目的と、規制主体の権限の関連について検討していく必要がある。さらに、ソフト・ローとして情報管理の高度な専門性の観点から ISMS 認証などによる評価基準を加味していくことも十分に考えられる。
【IT 統制を含む内部統制整備に対する管理者責任】
次に、情報セキュリティ・ガバナンスにおける管理者責任のあり方について、会社法上の取締役責任を検討するにあたり、情報管理に特有な考慮事由を明らかにすることが重要であろう。とくに市場規制との関連では、重要なリスクが顕在化する前の管理責任と顕在化して損害が発生した後の損害賠償責任の追及については、異なるアプローチが必要になる。
わが国においても、取締役の内部統制整備に関する責任について既に多くの先行業績がみられるが、とくに IT 統制について特化して取締役の内部統制構築責任について論じたものはほとんど見受けられない。「財務報告に係る内部統制」に対する経営者の有効性の評価と、内部統制監査を要求する金融商品取引法はもとより、会社法上要請される内部統制の内容についても、会社法施行規則により規定される「リスク管理体制」、「情報の保管・管理体制」等の整備のなかに IT 統制が含まれていることは当然のことであり、これらが内部統制システムの一環として有効に整備されておらず、損害が発生した場合には、経営者らは善管注意義務違反として、その責任を問われる場合がある。
他方、このときの善管注意義務違反を検討する際に、経営者はその会社の意思決定プロセスが誠実かつ公正に確保されている場合には、著しく不合理な意思決定を行っていない限り善管注意義務違反を問われないという、判例法上の経営判断原則（ビジネス・ジャジメント・ルール）の法理の適用に配慮する必要がある。この経営判断原則が適用されるためには、会社の合理的

な意思決定プロセスにおいて一定の情報提供システムが整備されていることが不可欠の前提となる。今後、IT 統制は、この情報提供システムの整備の上で重要な要素となるものと考えられる。

この点においても、米国の州会社法上の内部統制に関する取締役の責任についての判例展開が一定の示唆を与えてくれる。デラウエア州の取締役の内部統制システム構築にかかわる取締役の監視責任について初めてその判断基準を提示した 1996 年のケアマーク判決が有名であるが、その後 SOX 法制定後には、事実上、上場企業の内部統制システムのレベルが向上しており、その構築義務違反の損害を株主代表訴訟において問われる場合、取締役に対する監視義務違反等の責任追及の方法について、Abbott　事件 (2003)、 Disney 事件 (2006)、Stone 事件 (2006) などに、変化の兆しがみられる。もとより、SOX 法は連邦の証券規制の一環として位置づけられており、SOX 法に基づく内部統制規制違反は、直ちに私訴権の対象とはならないが、SOX 法により有効な内部統制の構築が要請されているため、州会社法レベルでの訴訟においても株主による立証活動に対して貢献する側面がある。すなわち、SOX 法が要請する内部統制は、企業の規模や業種により、その具体的内容やレベルに経営者の裁量が認められているが、少なくとも、その内部統制が有効であるといえるためには、「財務報告に重大な虚偽記載を生じさせるおそれ」という重要な欠陥があったならば発見され是正されている状況であることが求められている。そうであれば、「内部統制が有効に機能している」と経営者が自己評価していたにもかかわらず、事後に内部統制に問題があったことが発覚し、損害が生じた場合には、重要な欠陥については取締役会において、取締役らに情報提供されていたはずである。したがって、その情報に基づいて是正措置を講じるなどの任務を怠ることがなかった点につき、取締役の側に挙証責任の転換が図られることになる。もとより、このときに十分な情報収集を行い、合理的な検討を加えたことが示されれば責任を免れることになるが、このときの内部統制上の問題について専門家らによる関与がどの程度図られたのか、会計問題であれば監査人、コンプライアンス問題であれば弁護士、IT 問題であれば IT 専門家らによる事前の関与が情報収集・検討の際にどれほど合理的なものであったかの説明責任が経営者側に課されることになる。こうした米国での判例法にみる変化は、我が国における会社法上の取締役の内部統制構築責任についても十分に参考となると考えられる。さらに今後、IT 統制については、それ以外の業務プロセスの統制とは異なり、適時性、共時性に配慮した対応がなされたかなどが、取締役の善管注意義務の履行の判断材料として重要になってくるものと思われる。

【まとめ】

以上のように、先行する米国の状況と比較しても、わが国の内部統制の要素である IT 統制が、会社の意思決定プロセスにおいて果たすべき役割と責任については、明確に示されていないのが現状である。しかし、少なくとも、こうした既存の法体系（ハード・ロー）である金商法、会社法の枠組みにおいて、その IT 統制に関わったそれぞれの立場の者の責任を問うために、各業種・業態の企業、およびその企業の自己評価に対する第三者の専門的評価主体（外部監査人・格付け機関・情報セキュリティ評価機関等）が、遵守すべきそれぞれの自主ルール（ソフト・ロー）の内容が、具体的な注意義務の判断基準の要素として採用されなければならないだろう。こうした法規制の柔構造化を採用することにより、時々刻々変化する情報セキュリティの状況を反映した規範を取り込む自主ルールに基づきながら、ハード・ローによる厳然たる責任を追及する法規制の運用が可能になる。他方、そうした事後的な救済の用意では対応しえない場面においては、事前の予防的エンフォースメントの充実を図る制度の確立が急務といえる。米国のようにインジャンクション、付随的救済による利益の吐き出し、民事制裁金、場合によっては資産凍結命令、役員の就業禁止などの対応はもとより、IT 統制上の問題の兆しがある場面において、米国 SEC が採用するようなアメとムチの方法により、リスクが顕在化する前に企業自らにその改善に向かわせるインセンティブ規制を確立することも重要である。このように、既存の法規制のなかに、機動的かつ柔軟な対応が可能な自主規制機関のルールを連動させることにより、情報セキュリティの特質に即したガバナンスの構築に貢献する規制となることが期待できる。

2　シグナル情報のあり方に関する提言

2.1　第三者認証制度に求められる８原則(鈴木)

第 2 編の 4 において、プライバシーマークの問題点として、①組織規定の不備、②指定機関と

付与機関の併存、③組織体制の未整備、④指定機関のばらつき、⑤費用の適正さの検証と会計監査の必要性、⑥不透明な不利益措置（注意、勧告、一時停止、取消し）が存在することを述べた。

民間団体が運営する第三者評価認証制度は、ブラックボックス化した制度内容が問題視されている。漢字検定協会などの問題が報道されたように、制度全体を真に監督する機能がなければ、ゆるやかに腐敗と惰性が支配するのである。昨今、ソフトローを評価する機運もあるが、それが法を補完する健全な社会的制度として機能しているか社会的にも評価する必要がある。やがて事業者のビジネスを不合理に制約を与える事実上の存在とならないためにも、民間認証制度の評価を行う社会的機能が必要であるように思われる。ここでは、その評価の基準となる８つの原則を提案したい。

私たちは、民間の第三者評価認証制度の社会的意義を確認するとともに、安易な第三者評価認証制度の濫立を抑止するためにも、また、消費者保護等公益的効果が乏しい制度のために経営の自由が過度に制約されることのないよう常に、第三者評価認証制度を点検し、評価し、必要に応じて、主催者への改善要求を行っていかなければならない。

制度を利用することは、制度への支持を社会的に表明することでもあるということを念頭において、取得するか否か、更新申請をするか否か、認証マークを返上するか否か、制度の廃止を求めるか否かなど、自ら考え、判断していく必要がある。問題は、認証マークが官公庁の事実上の応札条件となり、また民間事業者の購買等取引条件として提示されるなど各事業者の判断の自由を事実上奪う社会的構造が生じてきた場合である。適切な行政の関与と監督が求められるケースであるといわなければならない。それは、既に一定の社会的評価を得ているプライバシーマーク制度においても例外ではないだろう。

なお、以下の原則は、こうした趣旨を踏まえて作成した一つのたたき台である。

① 公益性の原則
公益性の原則とは、その制度が公益を目的としていること、現に公益の実現のために運営されていることをいう。

公益活動を継続していくため、第三者評価認証役務の対価等を徴収することは容認されるとしても、営利活動になってはならない。公益活動によって得た収入は、目的の実現と制度の維持に費消されるべきであり、目的外に費消されることはあってはならない。

プライバシーマーク制度でいえば、例えば、ライセンス料収入は個人情報保護活動にどの程度効果的に費消されているのか。利害関係者はその実態をどのように知ることができるのか、といったことが問われる。

② 独立性の原則
独立性の原則とは、審査機関とその監督機関とが独立していること、及び評価認証を行う機関とその評価基準を定立する機関とが独立していることをいう。

各組織は、意思決定機関が明確に定まっており、意思決定機関は、審査の申請事業者と直接の利害関係のない第三者的立場の者によって構成されていることが必要である。

プライバシーマーク制度においては、付与機関（監督機関）である JIPDEC が指定機関（審査機関）を行っていることは許されるのか。誰が評価認証や不利益措置の実質的に意思決定を行っているのか。意思決定機関を会長の単独制とすることは妥当か。現在ある JIPDEC の審査会の法的性質はどのようなものか、といったことが問われる。

③ 契約に基づく運営の原則
契約に基づく運営の原則とは、民間団体による第三者評価認証制度が、契約関係によって成り立ち、契約上の根拠に基づいて運用されなければならないということをいう。

この点は、法律に基づく行政庁の公証等と異なるところである。

プライバシーマーク制度においては、運営要領等契約に基づく運営が徹底されているかどうか。改正の根拠条項なく改正を繰り返してきたことの有効性を問わなくてはならないこと、プライバシーマークの取消（ライセンス契約の解除）等不利益措置の事由、判断基準が明確に契約内容として定められていないこと、JIPDEC の審査会の根拠規定が存在しないこと等を厳しく問うていくことが必要である。

④ 公開（透明性の確保）の原則
公開（透明性の確保）の原則とは、第三者評価認証制度に関する、契約の内容、審査機関の要件等、審査機関等主要機関を構成する要員の氏名・所属等、審査及び不利益措置等の基準、審査員の資格と登用の基準、監査の実施と報告書などを文書化し、誰もが等しくアクセスできるようにしなくてはならないということをいう。

プライバシーマーク制度においては、各種判断基準が十分に公表されているのか。審査会の構成メンバーの氏名や所属、その権限等について公表されているか、といったことが問われる。

⑤ 公平の原則
公平性の原則とは、第三者評価認証（申請書の受理、審査等）において全ての申請事業者が等しく取り扱われることをいう。

プライバシーマーク制度においては、審査契約における欠格事由の判断との関係において、ａ）反社会的勢力の排除、ｂ）欺瞞的な消費者取引を行っている事業者の排除、ｃ）十分な経営上の資力（信用）がない事業者の排除、ｄ）３名以下の小規模事業者などをどのように扱うかといったこととの関係で公平性が問われる。

公平性を担保する制度として、審査合否に対する不服、不利益措置の救済制度は十分か検討されるべきであろう。

⑥ 責任の明確化の原則
責任の明確化の原則とは、第三者評価認証が何を認証するものか、認証機関は、その認証について、誰に対しどのような法的、社会的責任を有するのかを明らかにすることをいう。

認証制度一般の問題だが、認証責任をどの程度負うのか明確にされているか、全てを免責とすることは第三者評価認証制度として許されるものなのかといったことが検討されなければならない。また、Ｆａｘ１枚の誤配信程度をあげつらうことが認証機関の役割と責任に基づくものなのか、制度目的などとの関係を含めて再検討が必要であろう。

⑦ 民主的関与の確保の原則
民主的関与の確保の原則とは、第三者評価認証制度の重要な基準の策定等について、当事者、関係者の運営への関与を確保しなければならないということをいう。

プライバシーマーク制度の評価基準として採用している JIS Q 15001 との関係でいえば、工業標準化法に基づき、工業製品に直接関わらない一般的な経営管理規格を定めること、国民の権利義務に関わる事項を定めることは、工業標準化法の趣旨に適合すると言えるのか。また、業者及び消費者団体等利害関係者は、JIS Q 15001 の制定過程にどの程度関与できるのか。プライバシーマーク制度における各種基準の作成過程に事業者及び消費者団体等利害関係者はどの程度関与できるかといったことも問われるべきだろう。

⑧ 専門性の確保の原則
専門性の確保の原則とは、第三者評価認証制度における契約や各種基準の作成、及び評価認証において必要とされる、法、技術、経営管理などの専門性を確保することをいう。

専門的な基準の策定等には外部の専門家が参加しその十分な助力を得る制度でなければならないという趣旨である。また、審査員の資格、その育成プログラムは専門的見地からも検証され、審査員のスキル要件を充たす者のみが認証業務に携わるよう運用されなければならない。

プライバシーマーク制度においては、JIPDEC 事務局内に法律の専門家がいるのか。実質的に、誰が基準を作成し、誰が認証し、誰が審査員の資格を認定しているのか。そのスキルはどのように担保されているのか。外部有識者（専門家）は、個々の判断にどの程度実質的に関与しているのかといったことが問われることになる。審査の指摘事項への異議、解釈の確認、再審査などの専門性に疑義がある場合の救済制度の充実なども検討されるべきだろう。

2.2 「見えないものの品質保証」に関する提言(林・田川)

【背景】

情報セキュリティにおいて守るべき対象は、情報資産であるとされているが、その中で「情報」

は大きなウエイトを占めている。従来は企業が保有する営業秘密、個人情報、知財情報などの機密性、完全性および可用性が、外部からの攻撃および内部や委託先からの故意や過失によって損なわれることが情報セキュリティ問題であったし、今後も重要な課題であり続ける。

このなかにあって、現在の企業の情報はコンピュータシステム、各種記憶媒体および紙媒体に蓄積されるとともに、情報ネットワークを流通している。加えて、企業の発信する情報がウエブサイトなどに、また、企業の発信情報に関する第三者のコメントなどがブログやSNSなどに存在し、多くの人々が容易にアクセスできる状態にある。このため、企業経営にとっては、自社が保有する情報だけではなく、自社の製品・サービスに関して自社が発信する情報や、自社に関して第三者が発信する情報の真正性も、重要な情報セキュリティ問題になってきている。

企業の提供する製品・サービスの品質については、企業と消費者等の間に「情報の非対称性」があり、グローバル市場経済化の進展に伴い、サプライチェーンがより長くなり、非対称性はさらに大きくなっている。企業が品質に関する情報（シグナル情報）を発信することで製品・サービスの品質保証を行うことは、情報の非対称性に起因する消費者の取引費用を軽減できる可能性があり、消費者の製品に対する信頼感や安心感を高めことが期待できる。このため、品質保証はマーケティングの観点からも有効であると考えられる。

法（ハードとソフト）による品質保証の仕組みとしては、法制度に加えて、A.品質に関して基準を定め、その基準に適合していることを認証する方式（ユーザに対しては付与されたマークを表示）、B.製品・サービスの提供者を有資格者に限定する方式、C.営業許可制、というような様々な方法がある。本提言では、Aの方式に関する品質保証に関して検討するが、現在の仕組みには問題点があり、消費者の信頼をむしろ損なう事象も発生している。

なお、本提言では、食品、消費生活用製品および住宅を先行事例として取りあげる。

【検討事項・視点】

(1)　現在の品質保証の仕組みは以下のようになっている。

①　品質保証の実効性を高める仕組み

（ア）　各分野で個別法がある。たとえば、食品分野では、食品衛生法、JAS法（農林物資の規格化及び品質表示の適正化に関する法律）、消費生活用製品分野では、消安法（消費生活用製品安全法）、PL法（製造物責任法）、住宅分野では、建築基準法、住宅品質確保法（住宅の品質確保の促進等に関する法律）、住宅瑕疵担保法（特定住宅瑕疵担保責任の履行の確保等に関する法律）などがある。

（イ）　これら諸法の理念を具体化するため、品質に関して基準を定め、その基準に適合していることを認証する方式（ユーザに対しては付与されたマークを表示）が一般化している。ここで代表的な方式として、第三者認証方式があり、法で指定された認定機関が登録（認証）機関を指定し、その機関が認証のための評価を実施し、合格すれば、製品に認証されたことを示す表示マークをつけることが許される。例：食品衛生法における食品表示（法19条）、JAS法における規格格付・品質表示制度、消安法におけるPSCマーク、住宅品質確保法における住宅性能表示制度

（ウ）　虚偽・過大な表示に対する法的措置が各法で規定されている。例：不正競争防止法（第2条13号の違反行為）、不当景品類及び不当表示防止法（第4条、第6条）

（エ）　製品に瑕疵・欠陥があり、ユーザに損害が発生した場合の法的措置が各法で規定されている。例：食品衛生法の販売等禁止（第7条、8条、17条）、消安法の危害防止命令（第３９条）、PL法の製造物責任（第3条）

（オ）　行政庁や認証機関が違反事業者に対して、報告の聴取、立入検査、などの他、登録取消、表示マークの使用禁止などを行う場合がある。

以上の仕組みは、法制度による品質保証の仕組みの規定、これに基づく第三者認証機関による認証制度および表示制度、この仕組みに対する違反行為等があった場合の罰則を含む措置による実効性の確保の仕組みという流れになっている。しかしながら、認証機関自体が正しい認証手続きを踏んでいなかったり、実製品とは異なった材料を使用した製品を認証時に持ち込んだりした事例も見られ、第三者認証制度自体の信頼性について疑問が投げかけられている事例も生じている。

②　ユーザに品質保証を「見える化する」仕組み

（ア）　表示についての基準が法で定められている場合がある。例：食品衛生法第 19 条

（イ）　製品に付与された表示マークが品質に関する一応の保証になっている。

（ウ） 設計標準使用期間および点検期間の設定および表示、点検等の保守サポート体制の整備を製造事業者に義務づける制度もある。（消安法の特定保守製品等点検制度）

(2) 品質を保証するという意味

品質保証とは、「確立した要求事項に適合する製品を提供できる能力があることを実証することによる信頼感の付与」であり、「品質要求事項が満たされるという確信を与えることに焦点を当てた品質マネジメントの一部（ISO9000 の定義）」（飯塚悦巧『ISO を超える』）とされる。（以下とつなげる）

しかしながら、品質マネジメントはその製品の製造プロセスに焦点を当てているので、表示と実態がかい離するケースとして、次の 4 つの場合があり得る。

① 食品偽装のように、表示自体が虚偽の場合。（表示者は知っていて故意に行っている。

② 適合性評価自体が適正に実施されなかったり、設定された基準自体に欠陥があって、 その結果、実品質と表示にかい離が生ずる場合

③ （品質管理マネジメントが不十分で）保証した品質を実現できずに、結果として表示が正しくなくなる場合。

④ 設定された基準・規格が適正であり、また、これに基づいて行われた適合性評価も適正に行われ、さらに品質マネジメントも適正に行われたにも関わらず、保証した品質が実現できず、被害が発生する場合

このように、どのような取組みをしても、リスクの顕在化をゼロにはできない。この問題を、品質保証と表示責任からどう考えるかが問題になる。

【提言】

① 企業の発信する表示情報による品質保証の仕組みは、マーケティングおよび企業に対する信頼性向上の観点から、経営上のリスク問題（すなわち当該企業のガバンナンスのあり方）としての位置づけを強化すべきである。

② 品質保証の仕組みは、企業、消費者、行政などのステークホルダー間のコラボレーション強化を通してその実効性が担保されるべきである。なぜならば、この仕組みは情報の非対称性を軽減するための仕組みであるので、究極的には、企業と消費者間での信頼感・安心感が高まることで、双方が利益を得るものであり、また、行政も取引の安全を強化することで、消費者利益を増進することができるからである。

③ 企業が品質保証に力を入れることに対するインセンティブを強化する観点から、市場における消費者の製品選択がより的確に行われるように、消費者に対する制度の仕組みの周知、表示と実態のかい離や製品欠陥による被害発生状況などに関する情報開示の強化、消費者の相談窓口機能の強化などの対策を強化すべきである。

④ 表示と実態が異なるケースとして 4 つのケースについて述べたが、それぞれにケースについての取るべき対策内容と手法が異なるので、ハードローとソフトローの仕組み、市場機能の活用など、適切な対策を使い分けるべきである。たとえば、食品偽装のような故意による虚偽表示に関するマイナスインセンティブとしては、公益通報者制度の活用や消費者の評判情報の収集・開示などが発見されやすい仕組みの強化、法的な抑制力の活用が考えられる。また、逸脱行為をしない方が利益につながるとのプラスのインセンティブとしては、市場機能の活用や企業のガバナンス強化が考えられる。

⑤ また、ゼロリスクはあり得ないことを考慮すれば、消費や利用に際して一定のリスクがあることを取扱説明書や製品自体に表示することも必要ではないかと考える。

⑥ 第三者認証制度における「第三者」がなぜ必要なのかについて、原点に回帰した議論が必要である。とかく、認証を求める企業と認証機関との関係に議論の関心が集まり易いが、重要なのは、企業と消費者との関係である。なぜなら「見えないものの品質可視化」は情報の非対称性を軽減する仕組みであり、十分な情報が得られない消費者の立場を強化するためのものだからである。

⑦ なお、この点に関する具体的原則については、「第三者認証制度における 8 原則」を参照されたい。

2.3 表示に伴う責任論（林・田川）

［背景］

2.2 の「見えないものの品質保証に関する提言」において指摘したとおり、有体物の取引にお

いても、その品質など「見えない」部分の識別については、提供者（企業）と消費者の間に「情報の非対称性」があることが多い。

e コマースが普及してネット取引が一般化すれば、有体の財貨に加えて、無体の財貨の取引も恒常的に行われるようになる。ここでは、「情報の非対称性」が有体物の場合以上に著しいことに加えて、取引が瞬時に完了しかつ不可逆（間違いがあっても、原状回復することができない）である。したがって、消費者保護の視点からも、取引コスト削減の視点からも、何らかの品質保証の仕組みが不可欠となる。

品質保証の仕組みとしては、A. 品質に関して基準を定め基準に適合していることを認証する方式、B. 製品・サービスの提供者を有資格者に限定する方式、C. 営業許可制、といった 3 つの方法がある。しかし、グローバル市場においては「自由競争」が原則である以上、A. の方式が望ましいことは言うまでもない。

A. の方式においては、財またはサービスの提供者がユーザに対して特定のマークを提示し、簡単に品質を見極めることができるような仕組みを取ることが多い。ここで、このマークを誰が付与しているかについては、① 自己宣言として提供者自身の判断で行う、② 民間の第三者機関が審査の上マークの表示を許諾する、③ 公の期間が検査などの手続きを経た上マークの表示を許諾する、といった３つのパターンがあり得る。しかし上記と同様、信用度は高める必要がある一方で、政府の介入は極力少なくするとの趣旨から、②の類型が一般化している。

また、これらの表示を偽ってマークの信頼度を毀損した提供者や、表示を信じて思わぬ被害にあった消費者に対して、誰（提供者、第三者機関、消費者など）がどのような責任を負うべきかが問題になる。

なお、ここでは以下に述べるような事情から、「責任」は sanction に相当するものとし、「法的責任」を超えた概念と考える。ここで sanction とは、「ある行為が社会的に許されないものである場合に、当該行為に対して採られる社会的にビルト・インされた対処策の総称で、制裁という負の側面と報奨という正の面の二面性を持つもの」と捉えている。

したがって、後述する responsibility、accountability、liability 等が、行為主体に着目した概念で、かつ個別具体的に適用が検討されるものであるのに対して、sanction は個別問題よりも抽象的な社会制度であり、行為主体は、いわば社会全体である。

本研究の検討過程では、かなり早い段階で私が「コミットメント責任」という概念を提起し、その実効性を検証するようメンバーを督励した（英語にすれば、sanction against commitment ということになろうか？）。これは、その後以下のように定式化されている。

「事業者が、情報管理を含む経営管理に関する約束事を、利害関係者に対して表示または情報開示したにもかかわらず、それに違反することによって生ずる広義の責任」

これは、責任の源泉を経営者等が行う「言明」に求める点で、会社法や金融商品取引法に基づいて、「内部統制報告書」で導入された方式を先取りしたものであった。内部統制報告書の仕組みは、2008 年の財務報告から本格的に実施された。その状況を精査した早稲田大学 GCOE「成熟市民社会型企業法制の創造」の調査では、「内部統制は有効に機能している」とする「経営者の言明」は、ほぼ 100％に近く、監査法人の「無限定・適正」の意見を得ている。

これをもって直ちに「コミットメント責任」の妥当性が証明されたということはできない。しかし、1 つの有力な事例、ということは許されよう。また民間のトレンド調査であるが、博報堂が 2010 年の動向として、『態度表明社会：賛成の連鎖が流れを変える』を世に問うたことも、大きな意味では「時流」を表しているものと思われる。

[検討事項・視点]

(1) インシデントの分類と責任

責任のあり方は、インシデントの種類によって大きく異なる。個人情報の漏洩では、故意の場合は当該漏洩者が、過失の場合は漏洩者の属する組織が、一義的な責任を負うべきであろう。この意味では、近代市民法の基本原理である「原因者責任」を、貫くことができる。

しかしスパム・メールのように、原因者を特定する費用が膨大であるとか、そもそも特定できない場合にも、「原因者責任」のみが対策であるとすれば、実効性はゼロに近い。そこで、従来の概念とは違うが、① 有効なフィルタリング・ソフトの開発者に報奨金を与える、② 自己責任でフィルターする、③ 保険に任せる、といった対策も併せて検討すべきであろう。

(2) リスク対策

リスク対策としては一般的に知られるように、① 回避する、② 低減する、③ 移転する、④ 受

容する、という 4 種類がある。上記のインシデントの種類ごとに、この 4 つの手段をどう組み合わせるのが有効であるかを、見極める必要がある。

(3)　責任の分類

責任を広義に捉える立場からは、① 主としてインシデント等に即応する場合の responsibility 、② 主としてインシデントの対外説明としての accountability、③ 法的な意味での liability の 3 種があるものと考えられる。法治国家である以上、③が最も重要であることは否めないが、先のインシデントの分類に見られるように、これだけでは十分ではない。

加えて、法の執行には時間と金銭的コストがかかる。ソフトローと呼ばれるような、業界の慣行や自主基準など、法そのものではないが法に近い機能を発揮している仕組みも活用する必要がある。その一例として、forward-looking accountability（将来に向けてのもので、「コミットメント責任」に近い）も検討の価値があると思われる。

(4)　責任の軽重

ソフトローに期待せざるを得ない事態は認識しつつも、個人情報の漏洩事故で見られたように、「誰も法的な責任は負わないが懲戒処分など実質的な罰は厳しい」(法的責任の希釈化と実質厳罰化）という事態は望ましくない。なぜなら、サンクションが不可視となり、萎縮効果が強くなるからである。責任の軽重が可視化され、「sanction のあり方」といった形で、横断的に比較して論議できることが望ましい。

(5)（主として法的責任の）実施主体

裁判（司法）に時間とお金がかかる現状から、行政により多くの役割を担ってもらうべきだという議論がある（白石)。他方で、それは「規制緩和」の流れに逆行するとの批判もある。実効性を重んじるのであれば、独立行政委員会のようなものを想定して、行政処分を前置し、段階的に法的措置が取られる方式が望ましい（アメリカの FTC の経験など＝柿崎)。

(6)　先行研究

柿崎　環「米国における SOX 法内部統制の現状と課題」上村達男（編著)『新法制の下での内部統制と企業経営』日本評論社（近刊）

川和功子「英国法における電子情報取引契約をめぐる契約法上の表示責任（上）（下)」『ＮＢＬ』No. 849、850（2007 年）

白石　賢『企業犯罪・不祥事の法政策：刑事罰から行政処分・社内処分へ』成文堂、2007 年

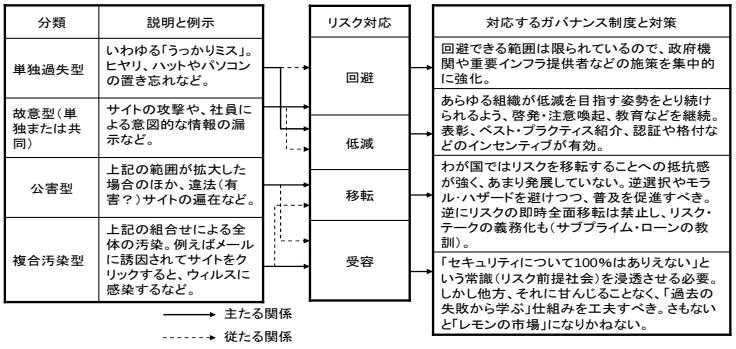
林紘一郎「見えないものの品質保証：第三者認証と責任」『日本セキュリティ・マネジメント学会誌』22 巻 1 号、2008 年

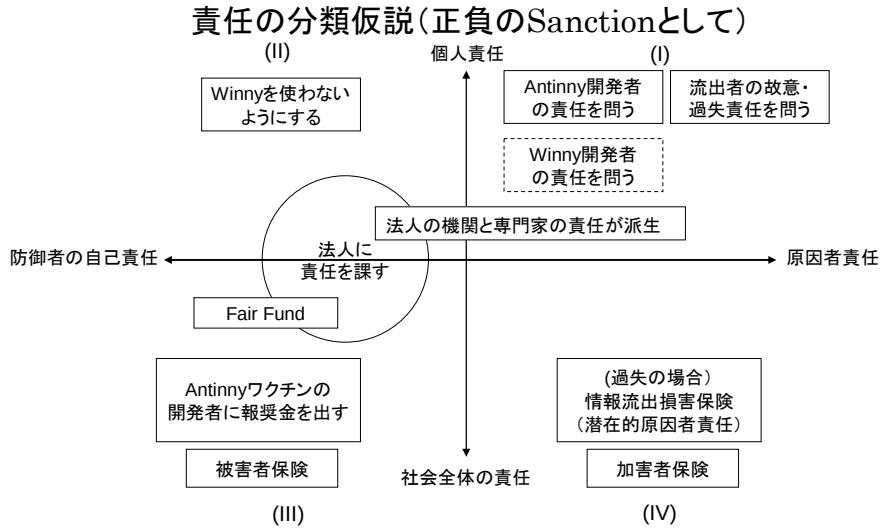
藤田寿夫『表示責任と契約法理』日本評論社、1994 年

(7)　現在の到達点

以上の考察を現時点で取りまとめて図表化すると、以下のようになる。

インシデントの分類とリスク対応とガバナンス制度





[提言]

① 中間報告で仮説として提示した「コミットメント責任仮説」は、本研究の過程で棄却されなかったので、さらに詳細な検討を続けるべきである。

② 上記仮説は、「内部統制報告書に対する経営者の言明」をモデルとしていたが、その実効性は「言明」が有効に機能したことで、間接的に証明された。今後も、同種の事例の実効性の観察を続けることで、社会全体に対する教訓を汲み取るべきである。

③ 「コミットメント責任仮説」は、景表法・不正競争防止法・JAS 法など法学の知見のほか、経済学における「レモンの市場理論」や「シグナリング理論」などとも関連性が強いので、学際的な研究として奨励すべきである。先行研究から読み取れるように、この分野の考察はきわめて乏しいので、研究者が関心を持って取り組むことを期待したい。

④ 法的責任のうち契約に書き込める部分は、SLA（Service Level Agreement）として具体化が望まれる。

3　情報と情報セキュリティの一般論に関する提言

3.1　企業における情報セキュリティの強化に貢献する法制度の実現に関する提言(鈴木・湯淺)

法制度班は、企業における情報セキュリティの強化に貢献する法制度の実現に向けて、現行の情報セキュリティ関連の法制度のうち特に国民の関心の高い個人情報の保護について、企業における個人情報の保護の実効性の確保という観点から既存法制と関連する諸制度について検討を加えてきた。

その結果、企業にとって過大な負担となっているためにかえって情報セキュリティの強化が妨げられている、実効性についての担保がないままに政府規制からソフトローにゆだねられた結果責任の所在が曖昧になっている、広範囲に伝播する情報の特性を無視して地方自治体に企業における個人情報の保護に関する義務を負わせている等の問題が生じ、既存法制及び関連する諸制度がかならずしも企業における情報セキュリティ強化に役立っていないことが明らかとなった。これらの問題点については早急に解決することが必要であり、下記に提案する方向性により法制度を改正することによって、企業における情報セキュリティの強化に貢献する法制度が実現するものと期待される。

3.1.1　プライバシー情報保護基本法の制定

企業における情報セキュリティに関する諸問題のうち、消費者および一般国民にとって大きな脅威となっているのは企業が保有する消費者等の個人情報の漏洩であり、個人情報の取扱いに関しては、個人情報保護法、自治体の条例、プライバシーマーク制度、ISMS など多様な手段によって個人情報の保護と適切な取扱の実現が図られることとなっているにもかかわらず、流出等の事例が相次ぐという事態になっている。その一方で、個人情報保護に関する過剰反応、個人情報保護を名目とした職場における労働者のプライバシー侵害等の問題も深刻となっている。

また地方自治体も個人情報保護法の規定により住民の個人情報の保護に関して責任を負い、近年各地の自治体において制定の動きが活発化している自治基本条例においても個人情報の保護をうたうものが多いことが本研究の成果として明らかになっているが[27]、広範囲に迅速に伝播するという情報の特性上、国の領土の一部である一定の地域を基礎とし、その地域内における住民を構成員としてその地域内における行政を行うことを目的とする自治体にとっては、その住民またはその地域内における個人情報の保護の徹底は到底困難であることが本研究の成果として明らかとなった[28]。

このことから、既存の個人情報保護法制に代わるプライバシー情報保護基本法の制定を提言する[29]。

現在、国内には、基本法と称する法典が 30 を超えるほど制定されているが、法令上、基本法についての定義規定は存在しない。衆議院法制局は国会答弁において、基本法とは、「国政の重要分野について進めるべき施策の基本的な理念や方針を明らかにするとともに、施策の推進体制について定めるもの」をいうと説明している。本提案では、「実質的な意味の基本法」を定義づけて論じていくというアプローチを採用する。実質的意味の基本法とは、憲法が全法秩序の最高規範として位置づけられその下にある全ての法律は、憲法の定める価値（人権）を具体化するものとして制定されているところ、その中にあっても、特に国会による明示的な憲法解釈としての性質を与えられ、人権規定を具体化しまたは補充することによって実質的意味の憲法の生成に寄与していくという法律である。

「プライバシー情報保護基本法」を制定する意義は、憲法上、「情報プライバシー権」が人権として保護されることを基本法において明確に宣言し、その内容を明らかにするとともに、人権を保障する具体的な仕組みを法律においても具体化するよう求めることにある。例えば、人権規定であるプライバシーの権利を根拠とした開示等請求権とその手続を定めること、行政の取り扱う国民のプライバシーに係る情報の取扱いについて主管する組織と独立した監査機関について定める。そのねらいは、第 1 に憲法上の「情報プライバシー権」から原理的に導かれる制約内容を明らかにすること、第 2 にそれを前提に行政の情報化を進展する環境を整備することである。

現行個人情報保護法制は、プライバシーとは何かという難度の高い議論をあえて回避し、プライバシーの権利を強く意識しながらも、それを明言することを避けることで起草されている。このため、再度、プライバシーの権利を軸に構成しなおすことも必要である。「情報プライバシー権」を補強する派生的な権利としてのデジタル化禁止権、データベース化禁止権、利用目的管理規制との関係で、データベース間の結合（横断的照合）禁止権、データベースへのアクセス（検索、参照、照合等）禁止権、または最近の RFID などの関係において、オンライン追跡調査（リアルタイム監視・記録）禁止権といったアイデアをどう立法政策に反映させていくか、現代の情報ネットワーク社会における病理現象を踏まえながら、現代的な日本法における「情報プライバシー権」を構想していかなければならない。その上で、「情報プライバシー権」の対象となる情報とは何か、「情報プライバシー権」の限界と調整法理について検討を加えることが求められている。

「プライバシー情報保護基本法」で確認すべき事項は、次の通りである。

①「情報プライバシー権」の定義と評価基準、監査基準の策定

②「個人情報」保護法制から「プライバシー情報」保護法制へー情報法（公法系）の再構成

③広範囲に伝播するため属地的に規制することが困難である情報の特性を踏まえ、個人情報保護や情報セキュリティ確保に関する国と地方自治体との役割分担の見直し

3.1.2　プライバシー・コミッショナーの創設

情報化の進展に対応するためには、国民を納得させるだけの大きな対応策を用意する必要がある。国民のプライバシー情報に係わる問題については、事後的ではあるが、裁判所の審査に期待することができる。しかし、司法は具体的な争訟事件につき、法を適用し、宣言することによって、これを解決する作用であるから、IT ガバナンス、マネジメントシステムのあり方、情報セキュリティ対策の内容について、詳細に分析する能力は乏しく、踏み込んだ判決を期待することに

---

[27] 湯淺墾道「自治基本条例の構造と動態」『九州国際大学法学論集』15 巻 2 号（2008 年）。

[28] 湯淺墾道「福岡県内の市町村における個人情報の保護に関する条例の現状と課題」『九州国際大学法学論集』13 巻 3 号（2005 年）、「自治体における個人情報保護 ―定額給付金・子育て応援特別手当の給付事務を中心に―」『九州国際大学社会文化研究所紀要』64 号（2009 年）。

[29] 詳細については、鈴木正朝「プライバシー情報保護基本法案の意義」東京財団政策提言『納税者の立場からの番号制度導入の提言』（2009 年）参照。

は限界があるといわなければならない。一方、国会については法案の審議は無論のこと、場合によっては、国政調査権などに期待できるが、従来の統治システムにおいては法案（閣法）提出前の起草段階での検討における国会の役割や関与は限定的であったことにも留意する必要がある。

このことから、プライバシー影響評価（Privacy Impact Assessment, PIA）の導入と、それを行う機関としてのプライバシー・コミッショナー機関の創設を提言する。

国民のプライバシー情報を活用した行政情報化の施策を講じる時は、その前に、計画段階で、国民のプライバシー侵害の影響（インパクト）の程度を評価（アセスメント）できるよう何らかの仕組み（ＰＩＡ）を導入することを検討すべきである。そのためには、国民から見て客観的立場でＰＩＡを行う信頼できる組織が必要であり、アセスメントの実施例やＥＵ諸国、オーストラリア、カナダなどのデータ・コミッショナー制度とＰＩＡの実施状況などを参考にすることが可能であろう。また米国では、2002 年電子政府法により連邦政府の全ての行政機関に対してＰＩＡの実施が義務付けられている。なお、現行の行政組織上は、個人情報保護法を主管する消費者庁がその任にあたるべきだということになろうが、その有効性についてはさらに検討を要するところである。

また、会計検査院にプライバシー情報の検査権の付与を行い、会計検査院の強化と活用を図るという方法も考えられる。プライバシーの権利に対する人権侵害の脅威については、統治機構に関わるレベルでの大きな人権保障の仕組みを提示することが必要である。

国家のＩＴガバナンスという視点からも、行政の国民情報の運用状況についての独立した監査機関はもはや不可欠であるといわなくてはならない。それは、総務省行政管理局による監督という行政内の統制に止まるものではなく、それとは別に、行政、国会、司法からも独立した会計検査院という憲法上の機関によって行われるべきである。会計検査院法を改正し、本来憲法の予定している強力な会計検査権を付与するとともに、あわせて法律上プライバシー情報に関する検査権を付与するという方法も検討に値しよう。実際の検査においては行政の保有する各種データベースを精査する必要があり、また適法な予算執行であるかどうかは、その施策の内容と離れて評価することはできない。日本とは異なる位置づけにはあるが、米国会計検査院（Government Accountability Office, GAO）のあり方は大きく参考にしていくべきであろう。

3.1.3 第三者認証制度の適正化（規律）

第三者認証制度は、認証機関が適切な事業を行う事業者を一定の基準により認証し、認証を受けた事業者にその旨を示す認定証やマークを付与してその使用を許可し、事業者が事業の実施にあたって認定証やマークを表示することによって、消費者に対して信頼できる取引相手であるかどうかの判断材料・基準を提供するものである。欧米では、トラストマーク制度が先行して導入された。認証機関（トラストマーク発行機関）の役割は、独立した機関として、特定の基準に合致した製品、プロセスまたはサービスを提供する事業者に対してトラストマークを交付することにある[30]。消費者保護の観点から注目されているADRとの関係では、トラストマーク制度はADRの普及を後押しするものとして評価されており、たとえば、2002 年にアメリカ法曹協会(ABA)が公表した電子商取引の紛争に関する最終報告書[31]においては、消費者の信頼を得る上で電子商取引事業者がトラストマークを取得することがきわめて有用であるとされている。わが国では、企業における個人情報保護に関する第三者認証制度としてはプライバシーマーク制度が広く普及している。

しかし 2007 年、プライバシーマークを取得していた大日本印刷株式会社が企業からダイレクトメール等の印刷物作成を委託されたところ、ダイレクトメールの宛先顧客の個人情報の一部が大日本印刷の業務委託先の元社員により不正に持ち出されて流出し、43 社分、8,637,405 件という大量の個人情報が流出するという事件が発生した。本件で問題となったのは、流出した個人情報の量の多さはもとより、プライバシーマーク取得の適正性と取り消しの是非であった。本件のような事例が発生した場合、事業者はもとより認証機関がどのような責任を負うのかは、「法的には誰も責任を問われない場合（「法的責任の希釈化」）と、法規範によらず他の社会規範で厳しく責

[30] Paolo Balboni, *Model for an Adequate Liability System for Trustmark Organization*, 1 INT. J. LIABILITY AND SCIENTIFIC ENQUIRY 151, 152 (2007).

[31] The American Bar Association, *Addressing Disputes in Electronic Commerce, Final Recommendations and Report of The American Bar Association's Task Force on Electronic Commerce and Alternative Dispute Resolution in cooperation with the Shidler Center for Law, Commerce and Technology, University of Washington School of Law* (2002). http://www.abanet.org/dispute/documents/FinalReport102802.pdf

任を問われる場合（「実質的厳罰化」）とが併存している」[32]とされ、当該事業者の個人情報の取扱い・保護が適正であると認証した認証機関自体の法的責任については、個人情報を流出・漏洩させた事業者の法的責任以上に不透明である。またトラストマーク制度に関しては、先行したヨーロッパやアメリカにおいても多くの問題点が存在している。中でも大きな問題となっているのは、トラストマーク類の乱立[33]と、トラストマーク制度の導入が消費者のインターネット上の商取引に対する不安感や不信感の解消に必ずしも役に立っていないという点である。

いっぽう、トラストマークは政府系の機関が認証機関になっている場合もあるものの、民間企業が認証機関となっている場合が多く、表示にあたって必ずしも法的規制を受けるわけではない。この点で、農林物資の規格化及び品質表示の適正化に関する法律（JAS 法）に基づき農・林・水・畜産物およびその加工品の品質保証の規格に適合した食品等の出荷・販売の際に付することが認められている規格証票（JAS マーク）などとは性質が異なる。にもかかわらず、官公庁の情報システム等の調達仕様書や入札説明書においては、プライバシーマークの取得が入札の条件になっている場合が少なくない。このため、プライバシーマークの取得自体に法的強制力はないものの、プライバシーマークを取得することは事実上情報システム関係の事業者にとって必須となっている。このため、プライバシーマークを取得する企業からみれば、当該マークの表示に対して消費者が個人情報の取扱い・保護に関する一定の信頼を置くことが期待されそれが取得のインセンティブの一部になるというトラストマーク本来の意義をこえて、プライバシーマークの取得が事実上義務化しつつあるといってよい。現時点では、トラストマークは事業者を推奨したり、事業者が提供する商品・サービス等の内容・品質を保証したり、事業者の経営内容を保証したりするものではないことを明記する必要があると考えられるが、結果として、第三者認証制度は企業における情報セキュリティ、個人情報保護の強化に本当に寄与しているかという疑念が広く共有されるようになったのが現状であろう

これらの事情をふまえて、第三者認証の適切な運用を行うための法制度の確立と規制の実施を提言する。

法制度の確立にあたっては、欧州委員会が 2000 年 5 月に消費者団体と企業の代表者などからなる「電子信頼イニシアティブ(e-confidence initiative)」を組織し、ヨーロッパ消費者連合(BEUC)とヨーロッパ事業者連合（Union of Industries of the European Community = UNICE）の協働により「ヨーロッパトラストマーク要件（European Trustmark Requirement = ETR)」を取りまとめて公開した[34]ものが大きな参考となろう。ETRでは、次の事項を定めている[35]。

1　トラストマーク制度の目的
2　消費者・事業者双方に対して透明なトラストマーク制度の運用
3　消費者・事業者双方がアクセス可能で可視的なトラストマーク制度の運用
4　トラストマーク制度の射程と内容
・言語
・商業上の表現及び公正なマーケティング
・児童
・契約前情報
　総則、財やサービスに関する情報、契約情報、その他の情報、注文確定プロセス、契約上の行為、支払い、セキュリティ、データ保護、苦情申し出と ADR 等
5　トラストマーク制度の運用
6　トラストマークの申請者の調査
7　モニタリング
8　実施システム
9　技術的セキュリティ

特に ETR では、第三者認証機関自身に対する規定を定めており、トラストマーク認証機関に対

---

[32] 林紘一郎・鈴木正朝「情報漏洩リスクと責任―個人情報を例として―」法社会学 69 号（2008 年）147 頁。
[33] EU 諸国におけるトラストマーク類を概観するものとして、Jan Trzaskowski, *E-Commerce Trustmarks in Europe : An Overview and Comparison of Trustmarks in the European Union, Iceland and Norway*, Report, European Consumer Centre Denmark (2006). http://www.legalriskmanagement.com/PUBLICATIONS/2006_TRUST.pdf
[34] The European Consumers Organization, *UNICE BEUC e-Confidence project* (2000). http://legacy.quatro-project.org/files/file/unice-beuc/eConfidence.pdf
[35] 湯淺墾道「個人情報の漏洩事例と認証機関」『九州国際大学法学論集』16 巻 2 号（2009 年）。

するガイドラインとなる内容にとどまらず、独立第三者機関によってトラストマーク認証機関の認証と監視を行うこと、認証したトラストマーク事業者の活動を年度報告書ベースで監視すること、独立第三者機関の審査を含めてトラストマーク事業者の認証と監視スキーム全般についての責任を負う機関としてBEUCおよびUNICEから選ばれた同数の委員と有識者委員により構成される電子信頼委員会(e-confidence commission)を設置することが盛り込まれた。EU 全体での ETR によるトラストマーク規制の導入は実現しなかったが、現時点ではイギリス、ドイツ、オーストリア等の一部の加盟国で国が一定程度の介入を行うか、ETR と同様のスキームによってトラストマークの認証を行う仕組みが導入されている。

わが国において認証機関の信頼性を高めるための法制度を策定する場合には、法規制に盛り込むべき内容としては、EU における ETR の例などに徴して、少なくとも認証機関自身が以下の要素を備える必要があることを明記すべきであると考えられる。

①認証機関の独立性
②審査過程の公平性
③認証を受けた事業者に対する積極的なモニタリング
④認証機関の執行力（違反事業者の調査と制裁）
⑤認証機関自身のアカウンタビリティ、認証機関自体を公的に認証する仕組みの確立

3.2 情報法の客体としての「情報」の捉え方に関する提言(林)

[背景]

「情報法」という名を冠した書物が 30 冊に近く、同様の名の大学での講義科目も、今日では珍しいものではない。しかし、このことが「情報法」という法領域がほぼ確定され、研究者の間で共有された結果だ、とまでは言いにくい。

なぜなら「法学入門」なら、これを講ずる教師の間にある程度の共通認識があると思えるが、「情報法入門」がそこまでの共通理解を得ているとは言えないからである。現状はなお、「群盲象を撫でる」に近い、というのが実感である。

この現状を打破するためには、情報法の研究者がそれぞれ独自に考えてきた「情報法」の成果を持ち寄り、「情報法の基礎理論」といったテーマについて、共同で討議する場が不可欠だし、そろそろ可能ではないかと思われる。

ここで、「情報法の基礎理論」を構成する主な要素は、他の法分野と大差なく、①客体論（情報法で保護または禁止される客体とは何か)、②主体論（情報主体とは誰か、自然人と法人のほか、センサーなどの機械をどう捉えるか)、③行為論（情報に関する主体の行動のうち、法的な効果が付与される行為とは何か）④手続論（情報を対象にする法には、どのような手続きが必要か）の 4 つである。

なお当研究会では、初期の段階で「情報セキュリティ基本法」をテーマにしたらどうか、という検討が行われた。その結果は、情報セキュリティ法とは結局のところ「情報」をどう保護（禁止）するかの問題に帰着するので、「情報法の基礎理論」（特に客体論）の検討なしで基本法を作っても、それは理念を述べただけで実効性はおぼつかない、という暫定的結論であった。この意味では、本検討は「情報セキュリティ基本法」にいたる道筋の第一歩、と言い直すこともできる。

[検討事項・視点]

(1) 従来の「情報」の保護方式

これまで「情報」として法的保護の対象になっていたのは、特定範囲の「秘密」と、「知的財産」として法定されたものの 2 種類に限られ、それぞれが不十分であるだけでなく、その間に共通項はなかった（これらを通底する基本法はなかった)。後者については、知的財産基本法が制定されたものの、多数の個別法を網羅しただけで、「知的財産とは何か」という共通因子を抽出できいるとは言えない。

(2) 従来の「秘密」の保護方式

「秘密」が一般法によって保護されている部分は少なく、専ら個別の法に依っている。刑法は、医師・弁護士など特定の職業従事者の秘密の漏示と、信書を開封することを禁ずるにとどまり（刑法第 13 章 秘密を犯す罪)、「秘密」を一般的に保護する形式を取っていない。個別法には広範な秘密保護規定があるが、これらが整合が取れた形で立法され運用されているか否かは、はなはだ疑わしい（例えば、刑の軽重の合理性)。

一方、民法は主として有体物を対象にしているので（民法第 85 条「この法律において、『物』

とは有体物をいう。」)、無体の財貨の取り扱いは、主として知財法制に委ねられている。もっとも、名誉毀損などが不法行為を構成すれば損害賠償が認められるので、結果的に、「(名誉を毀損した」当該情報は禁止される」ことになる。しかし、こうした態様を「客体論」として扱う論者は少なく、専ら行為論として議論されている。

(3)「知的財産」の保護方式

知的財産のうち、特許・実用新案・意匠・商標など審査・登録といった方式を要するものは、権利の範囲がそれなりに明確で保護期間も適切である。しかし、著作権の無方式主義と権利の長さ（著者の存命中と死後 50 年）は、他の知的財産に対して異色の存在となっているのみならず、デジタル化によって実効性が危機に瀕している。なお、営業秘密は従来「知的財産型」とされてきたが、「秘密管理性」を要件とすることから、「秘密型」の保護だと考えると理解しやすい。

(4) 従来の「情報」の禁止方式

「わいせつ」など憲法でも保護されない情報があることは、古くから認められてきた。しかし、それを「情報」という保護（ないしは禁止）の客体として論ずることは少なく、「公然わいせつ」のように「行為論」として捉えることが多かったのではないか、と思われる。しかし「わいせつ物陳列罪」では、そうは行かず、「有体物」を客体として差し押さえなどの対象にせざるを得ない現状である。今後は、「情報」という客体の一種として再整理が必要になろう。

(5) 個人情報の保護

上記のような保護方式の欠陥に注意を喚起し、「情報を法的に保護することには、いかなる意味があるのか」を再認識させたのは、2005 年に全面施行された、個人情報保護に関する一連の法律であった。ここで目新しかったのは、従来の「秘密型」でも「知財型」でもない「個人情報」を保護するという点であった。いわば「第 3 類型」の保護方式を、無意識のうちに提案していたわけである。

しかし法の制定者にも執行者にも、そのような認識がまったくないままに法の施行を迎えたため、いわゆる「過剰反応」等の混乱が生じたのは、やむを得ないことであった。

(6) 2 次情報の扱い

さらに、シグナル情報を重視する本研究の結果からは、上記 3 パターンの情報のほかに、情報の品質等を示す「2 次情報」を保護することが、e コマースなどを発展させるためには不可欠である、との認識が示されている。

(7) 保護されるべき「情報」と禁止されるべき「情報」

以上を踏まえると、情報法の客体論として検討すべき「情報」は、次表のようにまとめることができる。

	客体	具体例
保護	1 次情報	秘密、知的財産、個人情報
	2 次情報	メタ（属性）情報、品質表示情報、検索結果？
禁止	時と場所と態様による	いわゆる有害情報
	いかなる場合にも	違法情報、ウイルス

(8) 注記

上表のうち、個人情報の保護方式としては、アメリカの著作権法に似た「限りなく人格権を捨象した著作権」に類似の方法が適切と考えているが、より詳しくは別項の「情報漏洩と個人データの保護に関する提言」を参照されたい。また検索結果の表示については、クローラーの情報収集の偏りと、表示画面の偏りについて、何らかの改善策が必要かと考えているが、詳細は別途検討したい。

[提言]

① 「情報法の基礎理論」に向かう第一歩として、「情報法の客体論」に関する研究者間の交流を促進すべきである。

② 客体を上記の表のように分類した上で、それぞれの対象について個別の論議を深めるべきである。

③ 個人情報について、「秘密型」「知財型」に続く第 3 類型として保護する方法について、衆知を集めるべきである。

④　情報は明確な移転もなく、一旦開示されたら取り返すことができない（取引の不可逆性）ので、実体法と同様かそれ以上に、手続法が重要である。差し止めなど、手続き的な検討を平行して進めるべきである。
⑤　別項で提言している「品質表示に伴う責任論」や「情報漏洩と個人データの保護」に関する提言などと、相互参照しつつ検討すべきである。

[参考文献]
林紘一郎「個人データの法的保護：情報法の客体論・序説」『情報セキュリティ総合科学』第 1 号、2009 年 11 月
林紘一郎・鈴木正朝「情報漏洩リスクと責任―個人情報を例として―」『法社会学』第 69 号, 2008 年 10 月

3.3　情報漏洩と個人データの保護に関する提言（林）

[背景]
個人情報保護法が全面的に施行された 2005 年以降、その保護に関する意識が高まり、マスメディアが積極的に漏洩事件を報道した影響もあって、一種のフィーバー状況を呈した。その有様は「過剰反応」と評される面が強かったが、他方で個人営業に近い小企業やベンチャー企業においては、こうした状況を意識しつつも、なおしばらくは「様子見」を決め込んでいる向きもある。
敏感に反応した諸企業は、情報セキュリティ・マネジメントシステム（ISMS）の認証や、個人情報保護マーク（P マーク）の取得に走り、その取得企業数は「うなぎのぼり」に上昇している。しかし、認証はプロセスを適切に管理しているか否かに関わるもので、認証を取得すれば事故が無くなるわけではない。現に、ISMS やＰマーク取得企業の中からも、個人情報の漏洩事故が続いている。
また、漏洩事件を起こした後の措置としては、不法行為による損害賠償訴訟が複数提起されたものの、その賠償額は巨額ではなく、訴訟参加者が少ないと予想される現状に照らせば、大企業にとって「リーガル・リスク」の必要を感じさせない程度である。
しかし他方で、大企業が一定数を超える漏洩事件を引き起こせば、マスメディアが殺到して、仔細にわたる情報開示や謝罪会見を求めるため、企業経営者にとっては無視できないリスクと認識され、「より安全」を求めて過剰なセキュリティ投資に向かっている気配が見逃せない。また、法的な責任追及が希薄な一方で、社内規定による懲戒処分や配置転換など、実質的には「厳罰化」が進んでいるのではないかと危惧されている。
そろそろ社会全体として、どの程度の保護レベルが望ましいかについての合意を得るべく努めなければ、「萎縮効果」が働いて企業経営がより「リスク回避的」になることが懸念される。もともと日本企業は、ベンチャーの起業率や成長率で先進諸国に遅れを取っており、「リスクを取りつつ安全措置も講ずる」といった気風に欠ける面があるからである。
[検討事項・視点]
(1)　企業のセキュリティ担当に聞けば、「情報セキュリティについては、個人情報保護が第一課題」という答えが返ってくるという状況は、「リスク・テーカー」として企業を捉えれば、「どこかがおかしい」のではないか。
(2)　企業の死命を制するリスクは他にもたくさんあるはずで、これらを冷静・客観的に評価する姿勢が望まれ、個人データについても「保護と利用のバランス」をより重視すべきである。
(3)　もともと個人情報が漏洩しても、人が死ぬわけでもないし、漏洩に伴う 2 次的被害については、現行法で十分対応可能なはずである（例えば、漏洩した個人データを元に詐欺が行なわれれば「詐欺罪」で対応する、というように）。
(4)　法律家は、自分の専門分野以外の事柄については、発言を控えることが多い。それは一面で、「法学者の謙抑的態度」として評価される面もある。しかし、先に分析したとおり個人情報保護方が、「秘密と知的財産」しか保護してこなかった「無形財」について、「個人情報」という第三の類型を新たに導入することを意味するなら、それにふさわしい議論を、専門分野を超えて戦わすべきである。
(5)　また、個人情報保護法を専門にしている学者は公法出身の学者が多いため、民間同士の商取引において、何が本当の問題なのかを正しく把握していない気味がある。こうした欠陥を乗り越えて、部分最適化ではなく「社会全体としての」最適化を図ることが必要である。

(6) マスメディアは本来的に、「人が犬に噛み付いた」といった、エキセントリックな話題に飛びつくものである。取材を受ける側も取材をする側も、また記事を読む側も、こうした限界をわきまえて対応する余裕が、必要である。
(7) 残念ながら法執行の現状は、「法の手続きは十分に守られているが、法の精神は忘れられている」というのが実態かと思われる。Rule（法律など権威あるものに規定された公準）ではなく Principle （Rule の下敷きになっている原理・原則）が守られるよう、法の見直しも含めた対応が望まれる。すべての出発点は個人情報保護法にあったのだから、これを抜本的に見直す点についても、革新的なアイディアが求められている。
(8) 個人データの保護について世界の流れは、個別法を優先させ、産業横断的一般法を持たないアメリカに対して、一般法を制定するのみならず「コミッショナー」のような行政上の責任者に規制権限を付与するヨーロッパが対立している。わが国は時の流れでヨーロッパ型に近くなったが、そのままで良いのか、もう一度立ち止まって考えるべきである。

（参考）個人データの保護に関するアメリカ・EU・日本モデルの比較

	USA	EU	Japan
Legal Tradition	Common Law	Statute	Statute
Official Norm	Sectoral Statute (State Laws)	Omnibus Directive	Omnibus Law + Administrative Guideline
Alienability (Propertization)	Alienable	Inalienable (not separable from privacy)	Inalienable (not separable from privacy)
Public/Private Dichotomy	Separate Treatment	Combined Principles + Separate Laws	Combined Principles + Separate Laws
Dispute Resolution	Litigation	Data Protection Commissioner	Mass Media

[提言]
① 個人情報保護法制は、特定の個人を識別できる「情報」を、当該個人からは離脱したものとして（アメリカ法的には alienable なものとして）取り扱うことを主眼としている。したがってその本質は財産権であり、人格権的救済は別途プライバシー侵害として保護することにして、財産権的取り扱いを徹底すべきである。
② この意味では、個人情報という用語は人格権的要素を彷彿とさせるので避け、「個人データ」という価値中立的な用語を用いるべきである。
③ その際、アメリカ法における著作権の扱いが参考になる。アメリカも 1989 年にベルヌ条約に加盟した以上、著作者人格権がないとは言えない立場になったが、依然としてごく一部を除いて人格権はなく、もっぱら財産権として運用されている。この実績を持ち込めば、個人データについて財産権的取り扱いに徹することは可能と考えられる。
④ かくして、個人データと（財産権部分だけの）著作物を、「秘密」と「知的財産」に続く「第 3 類型」として、情報法の保護客体にする道を真剣に考察すべきである。
⑤ 個人データの保護方式を考察することは、情報法の客体論の先駆的事例を扱うことと同じである。そこでの特色は、有体物の「一物一権」と違って、無体財については「一財多権」にならざるを得ないことで、これにふさわしい法制は未だ見出されていない。
⑥ 実定法の先例の無さを補っているのが、契約法における「ライセンス契約」である。知的財産に付随して生まれたものだが、次第に「新しく生成中の権利」についても、何らかの工夫がなされている。このエキスを吸収することで、制定法の要素が摘出できる可能性がある。
⑦ この検討には、「品質表示に伴う責任論」と「情報法の客体としての情報の捉え方」に関する提言が密接に関連するので、これらを総合的・包括的に検討すべきである。

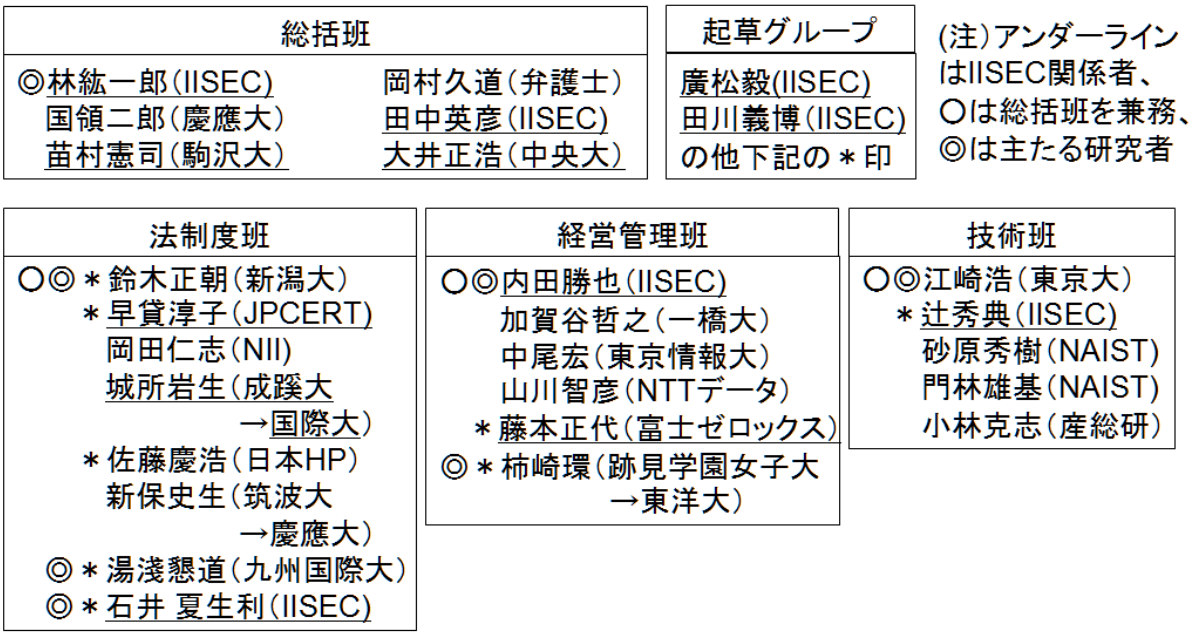
[参考文献]
林紘一郎「個人データの法的保護：情報法の客体論・序説」『情報セキュリティ総合科学』第 1 号、2009 年 11 月
Koichiro Hayashi, How to Protect Personal Data, Discussion Paper for Professor Lance Hoffman of George Washington University, November 17, 2009

林紘一郎・鈴木正朝「情報漏洩リスクと責任―個人情報を例として―」『法社会学』第 69 号，2008 年 10 月
椙山敬士『著作権論』日本評論社、2009 年。特に、第 3 部第 3 章

５．研究開発実施体制

(1)体制

2008 年度末までは、以下の分科会方式を採用し、2009 年度は、研究代表者林と起草グループが中心になって実施した。



(2)研究開発実施者

2008年度末までの研究開発実施者
①　総括班　*アンダーラインは情報セキュリティ大学院大学の関係者。

氏名	所属	役職	研究開発項目	参加時期
林 紘一郎	情報セキュリティ大学院大学	副学長・教授(当時)	全体の取りまとめ	H19.7～H21.3
岡村 久道	英知法律事務所	弁護士	同上	H19.7～H21.3
国領 二郎	慶應義塾大学	教授	同上	H19.7～H21.3
田中 英彦	情報セキュリティ大学院大学	研究科長・教授	同上	H19.7～H21. 3
江崎　浩	東京大学	教授	同上	H19.7～H21. 3
苗村 憲司	駒澤大学	教授	同上	H19.7～H21. 3
大井 正浩	情報セキュリティ大学院大学	客員教授	同上	H19.7～H21. 3

鈴木 正朝	新潟大学	教授	同上	H19.7～H21. 3
内田 勝也	情報セキュリティ大学院大学	教授	同上	H19.7～H21. 3

② 法制度班

氏名	所属	役職	研究開発項目	参加時期
鈴木 正朝	新潟大学	教授	法制度的観点から見た企業の「情報セキュリティガバナンス」と責任論	H19.7～H21. 3
早貸 淳子	JPCERT	常務理事	同上	H19.7～H21. 3
岡田 仁志	国立情報学研究所	准教授	同上	H19.7～H21. 3
城所 岩生	成蹊大学	教授(当時)	同上	H19.7～H21. 3
佐藤 慶浩	日本ヒューレット・パッカード株式会社		同上	H19.7～H21. 3
新保 史生	筑波大学(当時)	准教授	同上	H19.7～H21. 3
湯淺 墾道	九州国際大学	准教授→副学長・教授	同上	H19.7～H21. 3
石井夏生利	情報セキュリティ大学院大学	講師→准教授	同上	H19.7～H21. 3

③ 経営管理班

氏名	所属	役職	研究開発項目	参加時期
内田 勝也	情報セキュリティ大学院大学	教授	経営管理手法から見た企業の「情報セキュリティガバナンス」と責任論	H19.7～H21. 3
加賀谷哲之	一橋大学	准教授	同上	H19.7～H21. 3
中尾 宏	東京情報大学	准教授	同上	H19.7～H21. 3
山川 智彦	NTT データ		同上	H19.7～H21. 3
藤本 正代	富士ゼロックス		同上	H19.7～H21. 3
柿崎 環	跡見学園女子大学(当時)	准教授(当時)	同上	H19.7～H21. 3

④　技術班

氏名	所属	役職		参加時期
江崎　浩	東京大学	教授	技術的観点から見た企業の「情報セキュリティガバナンス」	H19.7～H21．3
辻　秀典	㈱情報技研	代表取締役	同上	H19.7～H21．3
砂原 秀樹	奈良先端科学技術大学院大学	教授	同上	H19.7～H21．3
門林 雄基	奈良先端科学技術大学院大学	准教授	同上	H19.7～H21．3
小林 克志	産業技術総合研究所		同上	H19.7～H21．3

2009年度の研究開発実施者

① 総括班　上記と同じメンバーである。

② 最終報告書起草グループ

氏　名	所　属	役　職	研究開発項目	参加時期
廣松毅	情報セキュリティ大学院大学	教授	最終報告書作成・取りまとめ	H21.4～H21.12
鈴木正朝	新潟大学	教授	最終報告書作成	H21.4～H21.12
早貸淳子	JP-CERT	常務理事	同上	H21.4～H21.12
佐藤慶浩	日本ヒューレット・パッカード㈱		同上	H21.4～H21.12
湯淺墾道	九州国際大学	副学長・教授	同上	H21.4～H21.12
藤本正代	富士ゼロックス		同上	H21.4～H21.12
柿崎　環	東洋大学	教授	同上	H21.4～H21.12
辻　秀典	㈱情報技研	代表取締役	同上	H21.4～H21.12
田川義博	情報セキュリティ大学院大学	セキュアシステム研究所　客員研究員	同上	H21.4～H21.12
石井夏生利	情報セキュリティ大学院大学	准教授	同上	H21.4～H21.12
成原　慧	東京大学大学院　情報学環・学際情報学府	博士課程2年生	同上	H21.4～H21.12

(3)招聘した研究開発協力者等

なし

6．成果の発信やアウトリーチ活動など

(1)ワークショップ等

年月日	名称	場所	参加人数	概要
2007年5月11日	情報セキュリティ・ガバナンス研究会フ	学士会館302号室	22名	法制度班、経営管理班からフィージビリティ研究会の成

	ィージビリティ総括会議			果、技術班からは活動予定の報告がそれぞれ行われ、今後の方針について意見交換を行った。
2007年11月29日	情報漏えいの責任はいかにあるべきか(シンポジウム)	情報セキュリティ大学院大学	63名	各班からの進捗報告に加え、上武大学大学院特任教授池田信夫氏による特別講演「情報セキュリティの経済分析」が行われた。
2008年3月24日	RISTEX全体報告会	同上	16名	最終報告書の目次案に関し、意見交換を行った。
2008年6月28日	企業不祥事とサンクションの有効性(シンポジウム)	同上	58名	首都大学東京教授の白石賢氏による特別講演「刑事処罰から行政処分・社内処分へ」のほか、「情報漏えいとコミットメント責任」、「スパムメール対策に関する総合的検討」をテーマにシンポジウムを開催した。
2008年10月27日	情報セキュリティガバナンス研究会全体会議	アルカディア市ヶ谷	11名	これまでの進捗状況及び中間報告結果、経済産業省「産業構造審議会情報セキュリティ基本問題委員会」WGにおける検討状況、SLAとセキュリティをテーマに全体で討論を行った。
2008年12月13日	情報セキュリティガバナンス研究会ワークショップ	弘済会館	約20名	「個人情報保護の新しい考え方」「検索エンジンの法的諸問題」をテーマに意見交換を行った。
2009年4月3日	情報セキュリティガバナンス研究会ワークショップ	アルカディア市ヶ谷	24名	情報セキュリティと「エンゲーメント」「ソーシャルキャピタル」に関する調査結果、企業ネットワークのトラフィック分析に関する調査結果等が報告され、意見交換を行った。

(2)論文発表（国内誌32件、国際誌1件）

① 2007年

・林 紘一郎「パネルディスカッション」(内部統制を中心に)法とコンピュータ第25号
・林 紘一郎「人間は間違えることを科学する」富士通総研Economic Review第11巻第4号
・湯淺 墾道「福岡県内の市町村における個人情報の保護に関する条例の現状と課題」九州国際大学法学論集第13巻第3号
・湯淺 墾道「マレーシアのサイバー法の近時の動向 －電子商取引法・電子政府行為法の制定を中心に－」九州国際大学法学論集第14巻第2号

② 2008年

・林 紘一郎「リスクとチャンス」情報通信学会誌第26巻第3号
・林 紘一郎・鈴木正朝「情報漏洩リスクと責任－個人情報を例として－」法社会学第69号
・林 紘一郎「見えないものの品質保証・第三者認証と責任」日本セキュリティ・マネジメント学会誌第22巻第1号
・林 紘一郎・石井夏生利「フォレンジックと実体法」日本セキュリティ・マネジメント学会誌第22巻第3号

・大井 正浩「日本企業に本当に必要な内部統制の実務」日本セキュリティマネジメント学会誌第 22 巻第 2 号
・大井 正浩「システム監査関連監査基準の統合」システム監査第 22 巻第 1 号
・湯淺 墾道「自治基本条例の構造と動態」九州国際大学法学論集第 15 巻第 2 号
・湯淺 墾道「リスクマネジメントと法制度」九州国際大学法学論集第 15 巻第 1 号
・柿崎 環「資本市場法制における内部統制システム―米国 SOX 法内部統制規制の最新動向を踏まえて―」(アカデミック・フォーサイト)会計・監査ジャーナル第 637 号
・石井 夏生利「情報セキュリティと専門家の責任」情報ネットワーク・ローレビュー第 7 巻
・石井 夏生利「情報セキュリティ監査人の責任」九州国際大学法学論集第 14 巻第 3 号
③ 2009 年
・林 紘一郎「地方公共団体と情報セキュリティ人材育成」月刊 LASDEC 第 39 巻第 3 号
・林 紘一郎「セキュリタイゼーションとセキュリティ」金融情報システム第 303 号
・林 紘一郎「『実学』とは何か：創刊の辞に代えて」情報セキュリティ総合科学第 1 号
・林 紘一郎「『個人データ』の法的保護：情報法の客体論・序説」情報セキュリティ総合科学第 1 号
・岡村 久道「IT リスクと法制度」情報ネットワーク・ローレビュー第 8 巻
・岡村 久道「情報ネットワーク法学会特別講演会 個人情報保護、自己情報コントロール権の現状の課題」NBL 第 912 号
・岡村 久道「実践！企業における適正な情報セキュリティ対策」ビジネス法務 11 月号
・大井 正浩「金融庁内部統制監査基準の性格と課題」日本セキュリティマネジメント学会誌第 23 巻第 1 号
・鈴木 正朝「経済産業分野を対象とするガイドライン 平成 21 年度改正案の解説」ビジネス法務 11 月号
・鈴木 正朝「プライバシー情報保護基本法案の意義」東京財団『納税者の立場からの納税者番号制度導入の提言』(第 4 章執筆)
・鈴木 正朝「個人情報保護法の潜在リスクに着目を」ファイナンシャルコンプライアンス 5 月号
・湯淺 墾道「環境モデル都市と法制度」九州国際大学社会文化研究所紀要第 63 号第 2 集
・湯淺 墾道「個人情報の漏洩事例と認証機関」第 16 巻第 2 号
・柿崎 環「内部統制―資本市場法と会社法の交錯」早稲田大学 21 世紀 COE 叢書『企業社会の変容と法創造 企業法制の現状と課題』
・江崎 浩「我が国のインターネットトラフィックの実態から見たネット中立性に関する問題点の考察」通信ソサイエティマガジン第 9 号
・佐藤 雅明、繁富 利恵、上田 憲道、党 聡維、植原 啓介、砂原 秀樹、村井 純「プローブ情報システムのためのプライバシを考慮した匿名認証方式の提案と評価」情報処理学会論文誌』第 50 巻第 1 号
・Atsuo Inomata, Satoshi Matsuura, Kazutoshi Fujikawa, Hideki Sunahara: "IT-Keys: New lecture style for Information Security", Proc. of IADIS International Conference Cognition and Exploratory Learning in Digital Age(CELDA2009),Springer, pp.784-785.
・猪俣 敦夫、東 結香、上田 昌史、砂原 秀樹「防護動機理論に基づく情報セキュリティリスク解明モデルの一検討」情報処理学会コンピュータセキュリティシンポジウム 2009 論文集第 1 巻第 11 号
・石井夏生利「プライバシー権の現在と未来－米国の最新の議論を踏まえて－」InfoCom REVIEW 第 47 号

(3)口頭発表（国際学会発表及び主要な国内学会発表）
①招待講演 （国内会議0件、国際会議0件）
②口頭講演 （国内会議6件、国際会議0件）
③ポスター発表 （国内会議0件、国際会議0件）

発表者 林紘一郎

タイトル　「無方式主義下の著作権登録制度」
学会名　日本知財学会第 5 回年次学術研究発表会
場　所　東京大学
日　時　2007 年 6 月

発表者　林紘一郎
タイトル　「情報セキュリティの「実効性ある」ガバナンスは可能か？」
学会名　日本セキュリティマネジメント学会公開討論会
場　所　中央大学駿河台記念館
日　時　2008 年 2 月

発表者　石井夏生利
タイトル「情報セキュリティと専門家の責任」
学会名　情報ネットワーク法学会第 7 回研究大会
場　所　新潟大学
日　時　2007 年 11 月

発表者　山川智彦
タイトル　「情報セキュリティインシデント対応に関する法的課題」
学会名　情報処理学会　第 42 回 EIP 研究会
場　所　同志社大学
日　時　2008 年 11 月

発表者　山川智彦
タイトル「演習ノウハウの活用による情報セキュリティインシデント対応プロセス確立についての検討」
学会名　情報処理学会　第 43 回 EIP 研究
場　所　敬和学園大学
日　時　2009 年 2 月

発表者　和泉順子、佐藤雅明、砂原秀樹
タイトル　「プローブ情報システムへの匿名性評価手法導入のための一考察」
学会名　第 45 回電子化知的財産・社会基盤研究発表会
場　所　新潟大学
日　時　2009 年 9 月

(4)新聞報道・投稿、受賞等

①新聞報道・投稿

・岡村久道「Q　流出した顧客名簿　使用止められる？」「A　強制は困難、違法性警告を」日本経済新聞 2009 年 5 月 18 日朝刊
・鈴木正朝「欠陥意識し論議開始を－－鈴木正朝・新潟大法科大学院教授に聞く」毎日新聞 2009 年 4 月 6 日朝刊（メディア欄）
・鈴木正朝「(コラム）一筆啓上・納税者番号制度　導入への課題」納税通信第 3086 号(2009 年 8 月 24 日）
・鈴木正朝「個人情報保護法：国民の知る権利、揺らいで４年半　見直しの課題」「行政機関対象の保護法見直しも　鈴木正朝・新潟大法科大学院教授（情報法)」毎日新聞 2009 年 11 月 2 日朝刊（メディア欄）
・藤本正代「社会制度と企業の情報セキュリティ管理」セキュリティ産業新聞(2008 年 11 月 25 日～2009 年 2 月 10 日、6 回連載）

②受賞　なし

③その他　なし

(5)特許出願

①国内出願（0 件）
②海外出願（0 件）

(6)その他の発表・発信状況、アウトリーチ活動など

①書籍、DVD など論文以外に発行したもの

・岡村 久道『情報セキュリティの法律』(商事法務、2007 年)
・岡田 仁志『電子マネーがわかる』(日経文庫、2008 年)
・林紘一郎・矢野直明『倫理と法―情報社会のリテラシー』(産業図書、2008 年)
・林紘一郎ほか『入門 情報セキュリティと企業イノベーション』(ジ アーズ教育新社、2008 年)
・岡村久道『個人情報保護法　新訂版』(商事法務、2009 年)
・岡村久道・森亮二『これだけは知っておきたいウェブ安全対策　インターネットの法律 Q&A』(電気通信振興会、2009 年)
・内田勝也「情報セキュリティに関するマネジメントシステムの維持管理についての管理・運用面に関する調査研究報告書(平成 20 年度ニューメディアを基礎とする調査研究事業)」((財)ニューメディア開発協会、2009 年)

②ウェブサイト構築

・リコー情報セキュリティ研究センターのウェブ・サイトの中に「情報セキュリティと法」というページを設け、情報セキュリティに関する主な法令の内容を解説している(2007 年 4 月以降順次掲載し、適宜コンテンツを更新中)。
http://www.rhc.co.jp/r-isap/column.html

③研究開発成果を発信するためのシンポジウム等の開催

・2007 年 11 月 29 日　情報セキュリティ大学院大学にて「情報漏えいの責任はいかにあるべきか」を開催
・2008 年 6 月 28 日　情報セキュリティ大学院大学にて「企業不祥事とサンクションの有効性」を開催
・2008 年 12 月 13 日　弘済会館にて「情報セキュリティガバナンス研究会ワークショップ」を開催
・2009 年 4 月 3 日　アルカディア市ヶ谷にて「情報セキュリティガバナンス研究会ワークショップ」を開催

④学会以外のシンポジウム等への招へいによる講演実施

発 表 者　林 紘一郎
タイトル `Content Filtering and Secrecy of Communications`
研 究 会　BHN Trainees
日　　時　2008 年 6 月

発 表 者　小林 克志
タイトル　Better End-to-End Visibility Leads Better Networks
会 議 名　3rd International Conference on Future Internet Technologies (CFI08)
場　　所　Seoul,
日　　時　June 20, 2008

発 表 者　林 紘一郎

タイトル「情報の保護と利用のバランス」
研 究 会　BHN Trainees
日　　時　2008 年 6 月

発 表 者　林 紘一郎
タイトル「米国はどこで道を誤ったか？ われわれはどうか？」
研 究 会　日本システム監査協会
日　　時　2008 年 6 月

発 表 者　林 紘一郎
タイトル　`Anonym,Pseudonym and Real Name:Some Thoughts on Privacy in the Net`
研 究 会　リコー・ヒューマン・クリエイツ株式会社
日　　時　2008 年 11 月

発 表 者　林 紘一郎
タイトル　パネルディスカッション「情報化社会の未来は開けるのか？」
会 議 名　第 25 回国際コミュニケーション･フォーラム(東京・秋葉原)
日　　時　2008 年 12 月

発 表 者　林 紘一郎
タイトル「情報セキュリティと経営者に求められる対応･責任」
場　　所　J パワーシステムズ(東京・銀座)
日　　時　2009 年 1 月

発 表 者　林 紘一郎
タイトル「リスクとチャンス」
場　　所　九州国際大学
日　　時　2009 年 1 月

発 表 者　内田 勝也
タイトル「ISMS の有効性の向上と認証審査」(基調講演)
　　「付加価値のある審査」(パネルコーディネーター)
セミナー名　情報マネジメントシステム認証機関協議会「ISMS セミナー 2009」
場　　所　パストラル(東京都港区)
日　　時　2009 年 3 月 3 日

7．結び

本プロジェクトに応募した背景には、以前から研究開発戦略センター(CRDS)で行っていた「情報セキュリティ総合科学」への取組を具体化したいという思いと、設立後間もない当大学院大学において、それを学問的に実現する方法論を見出したい(とりわけ技術分野に対して遅れている、社会科学分野の遅れを取り戻したい)という思いがあった。そのため、当初から対象範囲を広げすぎた面はあったものの、その意図に沿った成果を取得することもできた。

組織化にあたっては、総括班を入れて 4 つの班に合計 24 名という大所帯を抱えた。その結果、運営上のネックになった部分はあるが、多数の研究者と知り合いになった上に、各人の実力(得手と不得手)を知ることができた。最終年度には、各メンバーの得意分野と不得意分野を理解した起草委員会がイニシアティブを取り、停滞気味であった本研究を迅速に進めることができた。

土居領域総括からは、研究代表者のイニシアティブを期待するとのコメントをいただいたが、研究代表者としては、自分自身が一定レベル以上の「理論」に到達しない限り「分かった」という気持ちにならない傾向があり、強力なリーダーシップを発揮するに至らなかった点を反省している。しかし。最終年度にはこれまで以上に本研究のテーマに集中した結果、

「実学とは何か」「「個人データの法的保護」：情報法の客体論・序説」の論稿をまとめることができた。また、前記情報法の基礎理論の序説と、「日本的経営と情報セキュリティ」の関係について、ある程度の自信も生まれてきた。

これらを受けて、「法学「経済学」「経営学」という社会科学の 3 分野の理論をベースに、企業のニーズを踏まえつつ、社会全体に対する 9 つの「提言」をまとめることができたのは、本研究会における最大の成果であると自負している。今後は、本成果について、大学院の授業に取り組むなどしてわれわれの知識レベルを向上させるとともに、社会的な認知度の向上を目指していきたい。